METODOLOGÍA PARA LA CUSTODIA DE LAS ENTREVISTAS MILITARES DEL PERSONAL DESMOVILIZADO, DESDE LAS UNIDADES TÁCTICAS DE LAS FUERZAS MILITARES HASTA EL GRUPO DE ATENCIÓN HUMANITARIA AL DESMOVILIZADO

JOHN NEIDER OROZCO GÓMEZ
JOHN ALEXANDER LAMPREA HERNÁNDEZ

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2017

METODOLOGÍA PARA LA CUSTODIA DE LAS ENTREVISTAS MILITARES DEL PERSONAL DESMOVILIZADO, DESDE LAS UNIDADES TÁCTICAS DE LAS FUERZAS MILITARES HASTA EL GRUPO DE ATENCIÓN HUMANITARIA AL DESMOVILIZADO

JOHN NEIDER OROZCO GÓMEZ
JOHN ALEXANDER LAMPREA HERNÁNDEZ

Trabajo de grado para optar al título de
Especialista en Seguridad Informática

Director
ÁLVARO ESCOBAR ESCOBAR
MSc.

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2017

Nota de Aceptación

_____

_____

_____

_____
Firma presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá, D.C., Febrero de 2017

DEDICATORIA

A Dios todo poderoso por el don del aprendizaje y la inteligencia para captar todas las enseñanzas.

A nuestras familias por su paciencia y colaboración al permitir que le robáramos tiempo para lograr este objetivo

AGRADECIMIENTOS

Expresamos nuestro agradecimiento a:

La Universidad Piloto de Colombia, al cuerpo directivo de la especialización en especial al Ingeniero Álvaro Escobar, y al excelente cuerpo de docentes.

A nuestro asesor temático por su dedicación enseñanzas, lineamientos y paciencia.

A la Dirección de las Fuerzas Militares – Dependencia Grupo de Atención Humanitaria al Desmovilizado.

A todos los que de una u otra manera aportaron su grano de arena en la elaboración de este objetivo

CONTENIDO

pág.

INTRODUCCIÓN 14

1. FORMULACIÓN 15

1.1 PLANTEAMIENTO DEL PROBLEMA 15

1.2 JUSTIFICACIÓN 15

1.3 OBJETIVOS 16

1.3.1 Objetivo general. 16

1.3.2 Objetivos específicos 16

2. MARCO REFERENCIAL 18

2.1 MARCO TEÓRICO 18

2.2 MARCO INSTITUCIONAL 23

2.3 MARCO TECNOLÓGICO 32

3. DISEÑO METODOLÓGICO 34

3.1 HIPÓTESIS DE INVESTIGACIÓN 34

3.2 VARIABLES 34

3.2.1 Variables Independientes 34

3.2.2 Variables Dependientes. 34

3.3 METODOLOGÍA 34

4. ESTADO DEL ARTE DEL MANEJO DE LA INFORMACIÓN DE LAS ENTREVISTAS MILITARES DEL PERSONAL DESMOVILIZADO DEL GRUPO DE ATENCIÓN HUMANITARIA AL DESMOVILIZADO 36

4.1 FASE 1: LEVANTAMIENTO DE INFORMACIÓN 36

4.2 FASE 2: IDENTIFICACIÓN, ANÁLISIS Y VALORACIÓN DEL RIESGO FRENTE A LA INFORMACIÓN 38

4.3 FASE 3: RECOMENDACIONES ADMINISTRACIÓN DEL RIESGO 63

5. METODOLOGÍA PARA LA CUSTODIA DE LAS ENTREVISTAS MILITARES DEL PERSONAL DESMOVILIZADO 65

5.1 ALCANCE 66

5.2 CARACTERIZACIÓN DEL SISTEMA INFORMÁTICO 66

5.3 RESULTADO DEL ANALISIS DE RIESGOS 68

5.4 POLITICA GENERAL 68

5.5 MEDIDAS Y PROCEDIMIENTOS 69

5.5.1 Medidas 69

5.5.2 Procedimientos 70

6. PROPUESTA TÉCNICA PARA LA ADQUISICIÓN DE SOLUCIÓN ESPECIALIZADO QUE PERMITA EJERCER CONTROLES SOBRE LOS RIESGOS IDENTIFICADOS 74

6.1 BENCHMARKING 74

7. CONCLUSIONES 79

8. EFECTO TRANSFORMADOR DEL PROYECTO 81

BIBLIOGRAFÍA 82

ANEXOS 85

LISTA DE FIGURAS

pág.

Figura 1. Fuga comparativa 19

Figura 2. Magnitud daño Vs probabilidad de amenaza 39

Figura 3. Cuadrante mágico de gartner enterprise-network-firewalls 75

Figura 4. Cuadrante mágico de gartner DLP's 77

LISTA DE CUADROS

Pág.

Cuadro 1. Análisis de riesgo promedio 40

Cuadro 2. Matriz calificación y evaluación del riesgo 41

Cuadro 3. Análisis del riesgo - activo formato entrevista 41

Cuadro 4. Análisis del riesgo - activo equipo de cómputo para entrevista 42

Cuadro 5. Análisis del riesgo - activo entrevistador 43

Cuadro 6. Listado controles existentes 44

Cuadro 7. Matriz calificación y evaluación del riesgo 45

Cuadro 8. Criterios aplicabilidad controles 46

Cuadro 9. Desplazo matriz de calificación, evaluación y respuesta a los riesgos 46

Cuadro 10. Valoración del riesgo - formato informe entrevista - fuga información 49

Cuadro 11. Valoración del riesgo - formato informe entrevista - acceso no autorizado al formato del sistema 49

Cuadro 12. Valoración del riesgo - formato informe entrevista - alteración/modificación preguntas 50

Cuadro 13. Valoración del riesgo - formato informe entrevista - modificación información diligenciada ya ingresada 50

Cuadro 14. Valoración del riesgo - formato informe entrevista - destrucción 52

Cuadro 15. Valoración del riesgo - formato informe entrevista - plagio 52

Cuadro 16. Mapa de riesgos - activo formato informe entrevista 53

Cuadro 17. Valoración del riesgo - activo equipo de cómputo entrevista - acceso a dispositivos externos 54
Cuadro 18. Valoración del riesgo - activo equipo de cómputo entrevista - uso de equipos externos/personales 54
Cuadro 19. Valoración del riesgo - activo equipo de cómputo entrevista - uso de software no licenciado 55
Cuadro 20. Valoración del riesgo - activo equipo de cómputo entrevista - no uso de software antivirus/antispyware 55
Cuadro 21. Valoración del Riesgo - activo equipo de cómputo entrevista - no realización de mantenimiento 56
Cuadro 22. Valoración del riesgo - activo equipo de cómputo entrevista - retiro e ingreso de equipos de la institución 56
Cuadro 23. Mapa de riesgos - activo equipo de cómputo entrevistas 57
Cuadro 24. Valoración del riesgo - activo funcionario público/entrevistador - no existencia de actas 58
Cuadro 25. Valoración del riesgo - activo funcionario público/entrevistador - error en asignación de credenciales 58
Cuadro 26. Valoración del riesgo - activo funcionario público/entrevistador - suplantación/reemplazo no autorizado 59
Cuadro 27. Valoración del riesgo - activo funcionario público/entrevistador - amenaza/soborno/influencia externa 59
Cuadro 28. Valoración del riesgo - activo funcionario público/entrevistador - ausencia de personal capacitado 60
Cuadro 29. Valoración del riesgo - activo funcionario público/entrevistador - no existencia de unidad militar 60
Cuadro 30. Mapa de riesgos - activo funcionario público/entrevistador 61
Cuadro 31. Nueva matriz análisis de riesgo promedio 62
Cuadro 32. Fortalezas y precauciones presentadas en el informe “cuadrante de enterprise-network-firewalls 76

Cuadro 33. Fortalezas y precauciones presentadas en el informe "cuadrante de enterprise data loss prevention 78

LISTA DE ANEXOS

pág.

Anexo A. Ley 1581 de 2012 85

Anexo B. Ley 1621 de 2013 99

Anexo C. Decreto 857 – 2014 116

Anexo D. Ley 1712 de 2014 126

Anexo E. Informe entrevista GAHD 140

Anexo F. Auditoria y evaluación desmovilizados 164

Anexo G. Seguimiento y evaluación archivo 168

Anexo H. Matriz riesgo – activo formato evista 174

Anexo I. Matriz riesgo – activo equipo de cómputo para entrevistas 175

Anexo J. Matriz riesgo – activo entrevistador 176

Anexo K. Nueva matriz riesgo – activo formato informe entrevista 177

Anexo L. Nueva matriz riesgo – activo equipo de cómputo para entrevistas 178

Anexo M. Nueva matriz riesgo – activo entrevistador 179

Anexo N. Certificación avance proyecto GAHD – entrevistas 180

RESUMEN

Garantizar la preservación del secreto, la confidencialidad, la integridad y disponibilidad de la información suministrada en las entrevistas militares por el personal Desmovilizado, demanda al Grupo de Atención Humanitaria al Desmovilizado, programa del Ministerio de Defensa Nacional, el desarrollar una metodología para la custodia de las entrevistas militares del personal desmovilizado, desde las unidades tácticas de las fuerzas militares hasta el grupo de atención humanitaria al desmovilizado de acuerdo a la ley.

Como valor agregado a la metodología para evitar la fuga de información de las entrevistas militares del personal desmovilizado del GAHD, se debe garantizar la transmisión de forma segura y la divulgación de las responsabilidades legales y jurídicas de quienes interactúan en este proceso.

Es un hecho que se necesita que esta actividad tenga unos mecanismos de control que el GAHD y en su nombre las Fuerzas Militares tiene interés en poder establecer, mecanismos que bajo políticas y normas permitan cumplir con las medidas de protección de la información y sus activos.

Para tal fin, y con base en los conocimientos adquiridos en la Especialización de seguridad Informática, en la primera fase se realizó todo lo relacionado con verificación de procedimiento, política de seguridad del MDN, la ley de inteligencia y contrainteligencia, levantamiento de información, análisis y documentación de los elementos que interactúan en la entrevista; y en la fase dos se identificó y analizo el riesgo teniendo en cuenta la valoración de los activos y se realizaron recomendaciones con el fin de contrarrestar las fugas de información.

Del producto de estas dos fases, en la fase tres se elaboró la metodología para la custodia de las entrevistas militares del personal desmovilizado, la cual es una serie de actividades que tiene en cuenta aspectos normativos, tecnológicos, aspectos humanos y de entorno.

Esta metodología es un documento de trabajo y como tal será accesible a todo el personal que requiera su utilización por lo que la información que se incluye no es limitada o clasificada, su redacción es simple para que sea de comprensión de todos los involucrados en su cumplimiento y se ajustará en todo momento al sistema de seguridad diseñado e implementado por el MDN – DIR2014-18 del 19 de junio de 2014. Tendrá un carácter impositivo por lo cual se evitaron términos que no impliquen obligatoriedad y lo más importante deberá mantener el principio de mejora continua a partir de actualizaciones.

Palabras Claves: GAHD, MDN, metodología, riesgo.

INTRODUCCIÓN

En el presente documento se entrega la metodología para la custodia de las entrevistas militares del personal desmovilizado, desde las unidades tácticas de las fuerzas militares hasta el grupo de atención humanitaria al desmovilizado, la cual es de suma importancia para el proceso de reintegración a la sociedad de las personas que pertenecen a grupos armados organizados al margen de la Ley (GAOML). El principal objetivo en este proyecto es permitir la actividad de entrevistas con un componente fuerte de portabilidad y comunicaciones.

Como valor agregado a la metodología para evitar la fuga de información de las entrevistas militares del personal desmovilizado del grupo de atención humanitaria al desmovilizado (GAHD), se debe garantizar el envío de la información de un sitio a otro de tal manera que la persona que realiza la actividad, así como quien entrega la información deben saber que su actuar estará cobijado tanto legal como jurídicamente.

Es un hecho que se necesita que esta actividad tenga unos mecanismos de control que el grupo de atención humanitaria al desmovilizado (GAHD) y en su nombre las fuerzas militares tienen interés en poder establecer, mecanismos que bajo políticas y normas permitan cumplir con las medidas de protección de la información y sus activos. Por los diferentes sucesos en los que el uso indebido de esta información por gente inescrupulosa ha hecho que la organización militar pierda credibilidad y se debilite institucionalmente, es necesario el desarrollo de una metodología para la custodia de las entrevistas militares del personal desmovilizado, desde las unidades tácticas de las fuerzas militares hasta el grupo de atención humanitaria al desmovilizado, que garantice el principio de reserva a la población desmovilizada que demanda la ley.

1. FORMULACIÓN

1.1 PLANTEAMIENTO DEL PROBLEMA

¿El Grupo de Atención Humanitaria al Desmovilizado cuenta con una metodología para la custodia de las entrevistas militares del personal desmovilizado, desde las unidades tácticas de las fuerzas militares hasta el grupo de atención humanitaria al desmovilizado?

1.2 JUSTIFICACIÓN

Garantizar la preservación del secreto, la confidencialidad, la integridad y disponibilidad de la información suministrada en las entrevistas militares por el personal desmovilizado, demanda al GAHD, el desarrollar una metodología para la custodia de las entrevistas militares del personal desmovilizado, desde las unidades tácticas de las fuerzas militares hasta el grupo de atención humanitaria al desmovilizado de acuerdo a la ley.

Con base a la problemática que se viene presentando en Colombia, acerca de la aparición de hackers al servicio de personas que buscan por encima de todo favorecer su situación política para la obtención de beneficios propios, es necesario proteger la información sensible clasificada por el GAHD, como lo son las entrevistas de desmovilizados, las cuales son materia prima para definir la situación de esta población donde se mide la voluntad y la pertenencia, requisitos obligatorios para acceder a los beneficios del programa y del gobierno nacional, además también de ser un insumo necesario para el inicio de operaciones de desmovilización, donde se realiza un análisis de situación, para tratar de arrebatar la mayor cantidad de personal perteneciente a los grupos armados organizados al margen de la ley GAOML y la judicialización de los reclutadores de niños, niñas y adolescentes (NNA), disminuyendo así el enemigo y contribuyendo de esta manera a garantizar y agilizar el proceso de PAZ y por último insumo necesario para operaciones militares, logrando así el cumplimiento de la misión institucional y constitucional de las fuerzas armadas y de policía.

El proceso de desarme, desmovilización y reintegración de personas vinculadas con los GAOML, inicia con la valoración de las circunstancias del abandono voluntario y la pertenecía a un GAOML, mediante una entrevista que se realiza inicialmente en la unidad militar y/o policial donde se presente el desmovilizado y otra segunda entrevista que se realiza en los hogares de paz, sitio donde reside el personal desmovilizado con sus núcleos familiares e inicia el proceso psicosocial durante un lapso de 60 a 90 días.

Estas entrevistas se reportan mediante un documento, informe de entrevista el cual tiene una clasificación de reservado y contiene información exclusiva que permite constatar la pertenencia a un grupo armado ilegal y la voluntad de reincorporarse a la vida civil, y es enviada sin ningún tipo de seguridad o distribución a las oficinas del GAHD en Bogotá. D.C., en donde se recibe, se le da trámite y se le garantiza su debida custodia. Se aclara que esta entrevista no se constituye como medio de prueba para fines judiciales.

Estas fallas de confidencialidad, autenticidad, integridad y disponibilidad de la información, han permitido que documentos clasificados como reservados hayan sido encontrados en allanamientos a personas que nada tienen que ver con organismos militares o de policía como fue el caso del nombrado hacker Andrés Sepúlveda, a quien la fiscalía general de la nación le encontró al parecer entrevistas militares con el formato del grupo de atención humanitaria al desmovilizado GAHD y bases de datos con información de personal desmovilizado.

Otro aspecto que se viene presentando con este proceso de entrevista es la falsedad en testimonio y la facilidad para entregar al desmovilizado un libreto que por su contenido le permita al desmovilizado acceder a los beneficios que le ofrece el gobierno colombiano.

Por las fallas expuestas anteriormente, es necesario esta metodología con lo cual se podrá mejorar los procesos internos para el cumplimiento de la misión institucional y lo más importante garantizar el secreto al personal desmovilizado conforme a la ley; manteniendo al GAHD, con los niveles de seguridad mínimos requeridos que impidan la fuga de información de las entrevistas de desmovilizados.

1.3 OBJETIVOS

1.3.1 Objetivo general.

Diseñar una metodología para la custodia de las entrevistas militares del personal desmovilizado, desde las unidades tácticas de las fuerzas militares hasta el grupo de atención humanitaria al desmovilizado que garantice la preservación del secreto, la confidencialidad, la integridad y disponibilidad de la información suministrada en la entrevista militar por el personal desmovilizado.

1.3.2 Objetivos específicos

- Identificar, analizar y documentar los elementos que interactúan con la entrevista militar practicada al desmovilizado.

- Verificar el proceso actual de la entrevista militar practicada al desmovilizado.
- Plantear metodologías tecnológicas para la protección de información a través de mecanismos de cifrado.

- Plantear tecnologías para el almacenamiento de datos y supervisión de los mismos.

2. MARCO REFERENCIAL

2.1 MARCO TEÓRICO

Autenticidad, integridad, disponibilidad y confiabilidad son conceptos ligados al manejo de la información de forma segura, que garantizan la continuidad de los sistemas de información.

Según una de las definiciones de la RAE[1] para el termino seguro, es la de estar *libre y exento de todo peligro, daño o riesgo*, este concepto da pie a entender un sistema de información seguro como aquel conjunto de elementos organizados relacionados y coordinados entre sí, a los cuales a partir de la aplicación de unas normas, procedimientos, métodos y técnicas garantizan la mínima presencia de margen de riesgo.

En el mundo cambiante el disponer de información continua y confiable representa una gran ventaja. Desde que Francis Bacón acuño la expresión “la información es poder” han pasado más de 400 años y solo hasta nuestros días es cuando esta frase cobra mayor sentido. Tener información y saber cómo usarla es tener poder; se podría decir que la información es un activo que garantiza la continuidad operativa y como tal debe ser identificada por las personas que necesitan los datos

Según Johannes[2],La información cada vez más se convierte en la moneda real (no virtual) que representa los intereses de las empresas y sus credenciales para fundar nuevas posibilidades de mercados y oportunidades, que le permitan posicionarse y abrir nuevas fronteras en sus capacidades para crear movimientos disruptivos que afecten la estabilidad de sus sectores de negocio u otros emergentes. En este escenario, las prácticas de seguridad y control de la información no pueden seguir concentradas (exclusivamente) en los controles de acceso y deben evolucionar con la dinámica social propia de las organizaciones

El Paradigma de Seguridad está cambiando; ya no es sólo asunto de protegerse de las amenazas exteriores, ahora es cuidar la información que sale.

[1] REAL ACADEMIA ESPAÑOLA. Diccionario de la lengua española | Edición del Tricentenario. Seguro. RAE. [En línea]. [Consultado el 16 de enero del 2016]. Disponible en http://dle.rae.es/?id=XTrgHXd

[2] JOHANSEN, B. Leaders Make the Future: Ten New Leadership Skills for an Uncertain World. San Francisco, USA: Berrett-Koehler Publisher, 2009 150 p.

Para Sebastián Bortnik[3], Analista de Seguridad de ESET, la fuga de información se trata de un incidente que puede ser tanto interno como externo, y a la vez intencional o no. La información expuesta puede ser de cualquier índole: un listado de empleados con datos personales, listado de salarios, base de datos de clientes o una fórmula o algoritmo secretos; todos con un punto en común la información sensible en manos de terceros.

Es difícil medir el impacto de la fuga de información, pero puede ser muy diverso, especialmente según la intencionalidad del incidente.

Lo primero por lo cual se debe preguntar es por la magnitud de los eventos ocurridos, en cuanto a cantidad de registros robados y cantidad de incidentes ocurridos. Como se ve en la figura 1 tomada del informe publicado por Camilo Gutiérrez Amaya, Sr. Security Researcher de ESET; sin dudas es en los últimos años cuando se ha empezado a ver las fugas de información con mayores pérdidas de datos[4]

Figura 1. Fuga comparativa

Fuente: BORTNIK Sebastián. ¿Qué es la fuga de Información? – ESET. [En línea]. [Consultado el 16 de enero del 2016]. Disponible en: http://www.welivesecurity.com/la-es/2010/04/13/que-es-la-fuga-de-informacion/

[3] BORTNIK Sebastián. ¿Qué es la fuga de Información? – ESET. [En línea]. [consultado el 16 de enero del 2016]. Disponible en: http://www.welivesecurity.com/la-es/2010/04/13/que-es-la-fuga-de-informacion/

[4] GUTIÉRREZ Amaya, Camilo. 10 años de fuga de información: conoce los incidentes para no repetir la historia. – ESET. [En línea]. [consultado el 16 de enero del 2016]. Disponible en http://www.welivesecurity.com/la-es/2015/01/08/10-anos-fuga-de-informacion/

Un factor determinante en un incidente de fuga de información es la intencionalidad pues en estos casos el impacto es más claro: esa información puede ser utilizada para realizar un ataque a la organización, para venderse, para hacerse pública o para afectar la reputación o imagen de la organización, como fue el caso en el año 2014 de espionaje de la llamada "Operación Andrómeda[5]", del pirata informático Andrés Sepúlveda, y de la filtración de documentos secretos de inteligencia y de una supuesta lista de correos electrónicos de políticos y periodistas relacionados con el proceso de paz.

Esta información de ciudadanos colombianos tiene su primera normativa en el artículo 15 de la constitución política de Colombia[6]: Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley. Los funcionarios que abusen de las medidas a que se refiere este artículo incurrirán en falta gravísima, sin perjuicio de las demás responsabilidades a que hubiere lugar.

Pero más allá de la constitución por su expectativa de intimidad y por tratarse de datos personales y sensibles que afectan la intimidad del titular está información está protegida por la Ley 1581 del 17 de Octubre de 2012[7](ver anexo A): en especial el artículo 5 que habla de los datos sensibles que son los que afectan la intimidad del titular o cuyo uso indebido puede afectar su discriminación y dentro de los deberes de los responsables del tratamiento y encargados del tratamiento, plasmado en el artículo 17 numeral a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data; numeral d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento y numeral k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial para la atención de consultas y reclamos. De igual manera para los encargados del tratamiento.

---

[5] EL TIEMPO. Justicia; Operación Andrómeda. [En línea]. [Consultado el 16 de enero 2016]. Disponible en: http://www.eltiempo.com/politica/justicia/informe-militar-sobre-el-caso-andromeda/15141236.

[6] COLOMBIA. Constitución política de Colombia. [En línea]. [consultado el 16 de enero 2016]. Disponible en: http://www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-15.

[7] COLOMBIA. Alcaldía de Bogotá. Ley 1581 del 17 de octubre de 2015: Protección de datos personales. [En línea]. [Consultado el 16 de enero del 2016]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

La información de las entrevistas al personal desmovilizado al tener tintes de información de la intimidad personal y familiar y al contener datos sensibles que son los que afectan la intimidad del titular o cuyo uso indebido puede afectar su discriminación, también tiene una particularidad y es que esta información es de vital importancia para las entidades que llevan a cabo actividades de inteligencia y contrainteligencia como son las fuerzas militares y la policía nacional organizadas por éstas para tal fin, la unidad de información y análisis financiero (UIAF), la cuales están facultadas por la Ley 1621 del 17 de Abril de 2013[8] - Articulo 3, y que deben tratar esta información con calidad de reserva de acuerdo a lo estipulado en el Artículo 33 de la misma Ley: Por la naturaleza de las funciones que cumplen los organismos de inteligencia y contrainteligencia sus documentos, información y elementos técnicos estarán amparados por la reserva legal por un término máximo de treinta (30) años contados a partir de la recolección de la información y tendrán carácter de información reservada (ver anexo B).

Con la calidad de reserva legal entregada por el artículo 33 de la Ley 1621 del 17 de abril del 2013 (ver anexo B), el Decreto 857 de mayo 02 de 2014[9] en sus artículos 10 y 11 entrega niveles de clasificación a estos documentos que gozan de reserva legal así (ver anexo C):

Ultra secreto. Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar al exterior del país los intereses del Estado o las relaciones internacionales.

Secreto. Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar al interior del país los intereses del Estado.

Confidencial. Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar directamente las instituciones democráticas.

Restringido. Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información de las instituciones militares, de la policía nacional o de los organismos y dependencias de inteligencia

[8] COLOMBIA. Presidencia de la República. Ley 1621 del 17 de abril de 2013: Ley de Inteligencia y Contra Inteligencia. [En línea]. [Consultado el 16 de enero 2016]. Disponible en: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/2013/LEY%201621%20DEL%2017%20DE%20ABRIL%20DE%202013.pdf

[9] COLOMBIA. Presidencia de la República. Decreto 857 de 2104. [En línea]. [Consulta el 16 de enero de 2016]. Disponible en: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201712 %20DEL%2006%20DE%20MARZO%20DE%202014.pdf

y contrainteligencia, sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar en las citadas instituciones y organismos, su seguridad, operaciones, medios, métodos, procedimientos, integrantes y fuentes

Es también de mencionar que la información recolectada en el ejercicio de la entrevista del desmovilizado no puede ser considerada material probatorio de acuerdo a lo mencionado en el artículo 35 de la Ley 1621 del 17 de abril del 2013[10] (ver anexo B), pero su contenido podrá constituir criterio orientador durante la indagación. En todo caso se garantizará la reserva de la información, medios, métodos y fuentes, así como la protección de la identidad de los funcionarios de inteligencia y contrainteligencia.

Un actor importante en un sistema de información es el custodio y generador de la información, en este caso como todo el personal de las fuerzas militares de policía y demás organismos catalogados por la ley de inteligencia y contrainteligencia es considerado un servidor público, debe suscribir de acuerdo al artículo 38 de la Ley 1621 del 17 de abril del 2013[11] (ver anexo B) acta de compromiso de reserva en relación con la información de que tengan conocimiento. Quienes indebidamente divulguen, entreguen, filtren, comercialicen, empleen o permitan que alguien emplee la información o documentos reservados, incurrirán en causal de mala conducta, sin perjuicio de las acciones penales a que haya lugar.

Acciones penales consagradas en el código penal militar colombiano[12] Titulo V.

Delitos contra la seguridad de la fuerza pública, Capítulo III. De la revelación de secretos, Artículo 130 - Revelación de secretos: El miembro de la fuerza pública que revele documento, acto o asunto concerniente al servicio, con clasificación de seguridad secreto, o ultra secreto, incurrirá en prisión de cinco (5) a ocho (8) años.

Si la revelación fuere de documento, acto o asunto clasificado como reservado, el responsable incurrirá en prisión de dos (2) a cuatro (4) años. Artículo 131. –

Revelación Culposa: Si las conductas a que se refiere el artículo anterior se cometieren por culpa, la pena será de uno (1) a dos (2) años de prisión.

El manejo de esta información también está normalizado por la ley de transparencia, Ley 1712 del 06 de marzo de 2014[13], la cual en sus artículos 15 y 16 determina todas las obligaciones para que se tomen los programa de gestión documental en el cual se establezcan los procedimientos y lineamientos

[10]COLOMBIA. Presidencia de la República. Ley 1621 del 17 de abril de 2013. Op. Cit. p. 20
[11] Ibíd., p. 20
[12] COLOMBIA. Código Penal Militar. [En línea]. [consultado el 16 enero de 2016]. Disponible en https://encolombia.com/derecho/codigos/penal-militar/
[13] COLOMBIA. Ley de transparencia - Ley 1712 del 06 de marzo de 2014. [En línea]. [consultado el 16 de enero de 2016]. Disponible en http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201712%20DEL%2006%20DE%20MARZO%20DE%202014.pdf

necesarios para la producción, distribución, organización, consulta y conservación de los documentos públicos (ver anexo D)

Los repositorios de las bases de datos y archivos de inteligencia y contra inteligencia están regidos por la mencionado en el artículo 28 de la Ley 1621 del 17 de abril del 2013[14] el cual dice que se deberá tener un centro de protección de datos y archivos de inteligencia y contrainteligencia (CPD) y sus accesos deberán cumplir los criterios marcados en el artículo 12 de la misma ley (ver anexo B).

Es por esta normatividad y referencia que se hace necesario para el GAHD plantear una metodología para la custodia de las entrevistas militares del personal desmovilizado, desde las unidades tácticas de las fuerzas militares hasta el grupo de atención humanitaria al desmovilizado.

2.2 MARCO INSTITUCIONAL

Los antecedentes del Ejército Nacional de Colombia[15] se remontan a las décadas de 1770 y 1780 bajo la denominación de ejército comunero surgido en la actual región de Santander y Norte de Santander, liderado por José Antonio Galán.

En la gesta de la independencia, el 23 de julio de 1810, la junta suprema de gobierno recién creada dispone la creación del batallón de voluntarios de la guardia nacional compuesto por infantería y caballería, al mando del Teniente Coronel Antonio Baraya.

Con la independencia se forma la gran Colombia, durante este período el ejército se enfrentó a Perú venciéndolo el 27 de febrero de 1829 en la batalla del Portete de Tarquí. La gran Colombia contaba para mediados de los años 1820 con un ejército de 25.000 a 30.000 hombres, de los cuales alrededor de la mitad eran tropas regulares y el resto milicias.

En el año de 1886 se sanciona la Constitución Política de la República de Colombia donde se dispone que la Nación debiera tener para su defensa un ejército permanente, unificado y al servicio del poder regenerador. Por lo cual se aprueba un proyecto de ley para constituir el ejército nacional con dos divisiones, dieciocho batallones, una compañía suelta y medio batallón2.

La organización, composición, división, clasificación, jerarquía, mando y justicia militar de la fuerza pública era la dispuesta por el Código Militar de 1881 vigente

[14]COLOMBIA. Presidencia de la República. Ley 1621 del 17 de abril de 2013. Op. Cit. p. 21
[15] COLOMBIA. Fuerzas Militares de Colombia Ejército Nacional. Manual de Calidad, versión 8, 2015. [En línea]. [consultado el 24 de enero de 2016]. Disponible en https://www. ejercito.mil.co/?idcategoria=227258#

hasta 1915; según esta legislación los cuerpos del ejército se encontraban divididos en tres armas: infantería, artillería y caballería.

El 10 de octubre de 1896 se promulga la ley 35 para fijar un pie de fuerza pública permanente compuesta por 10.000 hombres de tropa, con sus correspondientes jefes y oficiales; este pie de fuerza representó una nueva reorganización del ejército en cinco divisiones y cuatro jefaturas militares.

Durante el siglo XIX, marcado por las constantes guerras civiles, surge la necesidad de tecnificar el ejército conllevando a la creación de la escuela militar en 1907 bajo la asesoría de la misión militar chilena; aparte de la dirección de la escuela militar, la misión chilena tuvo a cargo la reorganización del ejército.

Diversas misiones como la suiza, francesa y norteamericana influyeron en el actual carácter de la fuerza, se empezaron a considerar conceptos de operaciones conjuntas que permitieran incluir componentes fluviales y aéreos. En la guerra de Corea (1950-1953) participó el batallón de infantería N° 1 actuando dentro de la fuerza multinacional, quienes trajeron un nuevo modelo de organización para el ejército incluyendo estados mayores con sus secciones de presupuesto, inteligencia, organización, logística, personal y relaciones cívico militares.

Entre los años 1998 a 2002 se inició la reestructuración de las fuerzas militares contemplando la actualización de la doctrina militar, el fortalecimiento de la educación militar, la reorganización de la estructura militar para optimizar el control territorial, la profesionalización del ejército, reorganización de la inteligencia y contrainteligencia y fortalecimiento de los DDHH y DIH.

A nivel estratégico se crean las jefaturas de personal, operaciones, inteligencia y contrainteligencia, logística y acción integral; a nivel operativo se reorganizan las unidades operativas mayores, las unidades operativas menores, las escuelas de formación y capacitación, las unidades tácticas, técnicas y especiales[16]

El gobierno nacional, comprometido con el mandato constitucional del artículo 22 de la carta política[17], diseño el plan nacional de desmovilización.

El programa de atención humanitaria al desmovilizado del ministerio de defensa nacional PAHD, tiene como misión diseñar, implementar y brindar un servicio humanitario integral, transparente y de alta calidad para el desmovilizado y su grupo familiar que facilite su tránsito a la reintegración social y su difusión en el marco de las normas de derechos humanos y de derecho internacional humanitario.

---

[16] COLOMBIA. Fuerzas Militares de Colombia Ejército Nacional, Op. Cit. p. 21

[17] COLOMBIA. Procuraduría General de la Nación. Constitución política de Colombia. [En línea]. [Consultado el 24 de enero de 2016]. Disponible en: http://www.procuraduria. gov.co/guiamp/ media/file/Macroproceso%20Disciplinario/ Constitucion_Politica_de_Colombia.htm

Dentro del plan de acción del PAHD, como objetivos estratégicos se tiene, incentivar la desmovilización con énfasis específico en mandos medios y milicias urbanas, sensibilizar a la comunidad nacional e internacional, brindar y garantizar una atención humanitaria integral, eficiente y oportuna, prevenir el reclutamiento ilegal, para lo cual se han implementado diferentes acciones.

El programa de atención humanitaria al desmovilizado del ministerio de defensa nacional, ha sido responsable del diseño y ejecución de los mecanismos para incentivar a las personas, miembros de grupos armados al margen de la ley, a tomar la histórica decisión de abandonar las armas y desvincularse del conflicto, de forma individual, para acogerse a la primera fase del proceso de desmovilización formulado por el actual gobierno, dando cumplimiento al objetivo estratégico plasmado en el plan de desarrollo (Ley 812 de 2003)[18], cual es, brindar seguridad democrática y viabilidad al principio fundamental de los fines esenciales de un estado social de derecho (Democracia participativa y afianzamiento de la legitimidad del estado).

En ese orden de ideas, el programa (pieza clave de la política de seguridad democrática) ha asumido el reto de estructurar una adecuada atención humanitaria inicial para la población especial desmovilizada que son sujetos de la intervención diseñada dentro de la primera fase de su proceso de desmovilización. Dentro de los resultados obtenidos por la iniciativa de desmovilización que ha impulsado el gobierno nacional, se encuentra, el alto porcentaje de los desmovilizados atendidos actualmente quienes de manera individual han optado por una nueva alternativa de vida.

Es importante resaltar que la población desmovilizada representa un enorme desafío para el programa, puesto que exige fortalecer las intervenciones de carácter personal, familiar y social, que permitan a los excombatientes cumplir con los objetivos propuestos, dentro del término establecido para lograr un verdadero proceso de reintegración social y económico.

El gobierno nacional invita a los colombianos que hacen parte de las organizaciones armadas ilegales, niños y adultos, a abandonar las armas. Este programa, ofrece una alternativa viable y ágil para que inicien su vida, recuperen su núcleo familiar y abandonen definitivamente la clandestinidad. Pero este deber no es sólo un compromiso del estado y sus instituciones, sino también de la sociedad en conjunto: sector privado, las organizaciones civiles y la comunidad en general.

Contexto jurídico de la política de desmovilización y de reintegración

[18] COLOMBIA. Alcaldía de Bogotá. Plan Nacional de Desarrollo. [en línea]. [Consultado el 24 de enero de 2016]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=8795

- El artículo 22 de la constitución política señala la paz como un derecho y deber de obligatorio cumplimiento.

- Con la expedición del decreto 1385 de 1994 (modificado por el decreto 128 de 2003), se comenzó a abrir espacio para los insurgentes que decidieran deponer las armas en forma individual y voluntaria, creando el comité operativo para la dejación a las armas CODA, para verificar la pertenencia y la voluntad de abandono.

- La ley 418 de 26 de diciembre de 1997, prorrogada y modificada por la ley 548 de 1999, la ley 782 de 2002 y la ley 1106 de 2006, consagró unos instrumentos para asegurar la vigencia del estado social y democrático de derecho y garantizar la plenitud de los derechos y libertades fundamentales reconocidos en la constitución política y en los tratados Internacionales aprobados por Colombia.

- La norma anteriormente citada dispone que las personas desmovilizadas bajo el marco de acuerdos con las organizaciones armadas al margen de la ley o en forma individual podrán beneficiarse, en la medida que lo permita su situación jurídica, de los programas de reincorporación que para el efecto establezca el gobierno nacional.

- La resolución ministerial 0722 del 25 de mayo de 2001 creó el grupo para el programa de atención humanitaria al desmovilizado del ministerio de defensa nacional.

- El decreto 128 del 22 de enero de 2003 reglamentario de la ley 418 de 1997 en materia de reincorporación a la sociedad civil, entre otros aspectos que atañen a este programa, fija el procedimiento de la primera fase de la desmovilización; de conformidad con su artículo 1º, la política conducente a desarrollar el programa de reincorporación a la sociedad y los beneficios socioeconómicos reconocidos será fijada por el ministerio del interior y de justicia en coordinación con el ministerio de defensa nacional; define la conformación del comité operativo para la dejación a las armas CODA y establece sus funciones; advierte la competencia exclusiva del ICBF frente a la atención especializada requerida por los menores desvinculados del conflicto armado.

- El decreto 2767 de 31 de agosto de 2004 reglamentario de la ley 418 de 1997 en materia de beneficios económicos, por colaboración eficaz por parte de los nacionales colombianos, que individualmente y por decisión voluntaria, abandonen sus actividades como miembros de los grupos armados organizados al margen de la ley, y hayan demostrado, a criterio del gobierno nacional, su voluntad de reincorporarse a la vida civil con la connotación de ser certificados por el comité operativo para la dejación de las armas CODA.

Este decreto desarrollo, uno de los objetivos del ministerio de defensa nacional, cual es:

> Ejecución de políticas que logren incentivar mediante el ofrecimiento de beneficios económicos la entrega de cualquier clase de material de guerra, intendencia, comunicaciones o cualquier otro elemento que facilite a los grupos armados al margen de la ley el desarrollo de actividades ilícitas, así como el suministro voluntario y espontáneo de información por parte de aquellas personas que se acojan al programa de desmovilización y reintegración social a la vida civil del Gobierno Nacional.

Es importante ilustrar al despacho sobre los derechos económicos a desmovilizados derivados por la colaboración (entrega de información eficaz a la justicia y a la fuerza pública y de material de guerra, intendencia, comunicaciones o de cualquier otro elemento que facilite a los grupos armados ilegales el desarrollo de actividades ilícitas) para el pago de bonificaciones, lo cual se encontraba regulado en el decreto 128 de 2003, artículos 9 y 10, derogados por el decreto vigente 2767 de 2004 en concordancia con las directivas ministeriales 10 de 2003 y 24 de 2004 derogadas en su integridad por la directiva ministerial 16 de 2007, que establece el procedimiento y requisitos para el reconocimiento y pago de bonificaciones económicas a los desmovilizados certificados por el CODA, bien sea como ya se mencionó por entrega de información y/o material de guerra, intendencia y comunicaciones; sin embargo, estas directivas son aplicables dependiendo del estadio temporal en que tales actos hayan ocurrido y debiéndose previamente a su reconocimiento agotar una serie de exigencias en cada uno de los casos.

Este decreto 2767 establece bonificaciones económicas por los conceptos referidos en cabeza del ministerio de defensa nacional, es importante indicar que el procedimiento para el reconocimiento y viabilidad en el pago lo define la misma entidad de manera discrecional, a través de las directivas ministeriales ya citadas.

- La resolución 786 del 13 de junio de 2005, por la cual se reglamenta la prestación de ayuda humanitaria al desmovilizado por parte del ministerio de defensa nacional.

- La directiva ministerial No. 15 del 23 de julio de 2007, implementa la política de desmovilización del ministerio de defensa nacional, procedimientos que deben adoptarse y trato que debe conferirse al desmovilizado y a su grupo familiar.

Las funciones específicas del programa, se sintetizan así:

- Ejecuta las directrices que el ministro de defensa nacional imparta, a través del viceministro de asuntos políticos y temática internacional, para el cumplimiento de su objetivo.

- Apoya la elaboración por parte del comando general de las fuerzas militares y la dirección general de la policía nacional, de campañas de acción sicológica dirigidas a incrementar el abandono voluntario de los miembros de organizaciones armadas al margen de la ley.

- Vela porque al desmovilizado y a su grupo familiar se le brinde la atención y asistencia que requiera, cubriendo en todo caso sus necesidades básicas como son las de alojamiento, alimentación, vestuario, transporte y atención en salud.

- Coordina el traslado del desmovilizado desde el lugar de su entrega hasta el lugar en donde el PAHD pueda continuar brindándole atención y asistencia, según su disponibilidad.

- Expide al desmovilizado y a su grupo familiar, una carta provisional de salud.

- Procura que el período de tiempo durante el cual las unidades militares o de policía brinden atención humanitaria inmediata al desmovilizado y su grupo familiar sea lo más corto posible.

- Da aviso a la alta consejería para la reintegración social y económica de grupos y personas alzadas en armas en un término prudencial, sobre la recepción por parte del ministerio de defensa nacional de un desmovilizado.

- Propone y ejecuta medidas encaminadas a prevenir que personas intenten aprovecharse fraudulentamente de los beneficios ofrecidos por el programa de desmovilización y reincorporación a la vida civil.

- Entrega físicamente a la alta consejería para la reintegración social y económica de las personas y grupos alzados en armas, en un término no mayor de quince (15) días calendario, aquellos desmovilizados que hayan sido certificados como tal por el CODA.

- Organiza ciclos de conferencias y jornadas de capacitación que serán dictadas en todo el país a personal seleccionado, para optimizar el proceso de recepción de los integrantes de las organizaciones al margen de la ley que abandonan la lucha armada en forma voluntaria.

- Difunde la legislación vigente sobre el proceso de desmovilización y reintegración social y económica.

– Propone medidas encaminadas a facilitar y optimizar el cumplimiento de los objetivos del PAHD.

– Vela por la transparencia en la gestión de los recursos asignados al ministerio de defensa nacional para el desarrollo de los objetivos de la política de desmovilización y reintegración social y económica.

– La ley 975 del 25 de julio de 2005, conocida como ley de justicia y paz, tiene por objeto facilitar los procesos de paz y la reincorporación individual o colectiva a la vida civil de miembros de grupos armados al margen de la ley, garantizando los derechos de las víctimas a la verdad, la justicia y la reparación.

Esta ley consagra un procedimiento jurídico especial, aplicable a las personas vinculadas a grupos organizados al margen de la ley, como autores o participes de hechos delictivos cometidos durante y con ocasión a la pertenencia a esos grupos antes del 25 de julio de 2005, que hubieran decidido desmovilizarse, tales como, los grupos de guerrilla o de autodefensas.

La connotación jurídica radica en que, quienes no pueden acceder a los beneficios jurídicos previstos en la Ley 782 de 2002, se les aplicará este procedimiento jurídico especial, por delitos diferentes a los políticos denominados atroces.

La finalidad es someterse a la VERDAD, JUSTICIA Y REPARACIÓN.

– El decreto 3043 de 7 de septiembre de 2006, ordena en el departamento administrativo de la presidencia de la república, la creación de la alta consejería para la reintegración social y económica de personas y grupos alzados en armas, que tiene dentro de sus funciones señaladas en el artículo 2°, entre otras, la de diseñar, ejecutar y evaluar la política de estado dirigida a la reintegración social y económica de las personas o grupos armados al margen de la ley, que se desmovilicen voluntariamente de manera individual o colectiva, en coordinación con el ministerio de defensa nacional, el ministerio del interior y de justicia y la oficina del alto comisionado para la paz.

– El decreto 395 de 14 de febrero de 2007, reglamentario de la ley 418 de 1997 y modificatorio parcialmente del decreto 128 de 2003, prevé en su artículo primero que los beneficios, que en el marco de la reintegración, reciban las personas desmovilizadas, a partir de la vigencia del citado decreto 128, de grupos armados organizados al margen de la ley en forma individual o colectiva, podrán concederse a cada persona, de acuerdo con los criterios que previamente determine la alta consejería para la reintegración social y económica de las personas y grupos alzados en armas, y terminarán cuando culmine el proceso de reintegración social y económica, el cual se fijará a partir del progreso de cada persona. De igual manera, establece el proceso de recepción del desmovilizado

que se entrega de manera individual y voluntaria y ordena que los programas de difusión para incentivar la desmovilización de miembros de los grupos armados ilegales, estén a cargo del ministerio de defensa nacional.

– La directiva ministerial No. 16 del 23 de julio de 2007, implementa la política, procedimientos y controles internos para el reconocimiento y pago de bonificaciones a los desmovilizados certificados por el CODA, por concepto de colaboración, por entrega de información y de material de guerra, intendencia o comunicaciones o cualquier otro elemento que facilite el accionar delictivo de los GAOML.

Dentro de las condiciones para la operatividad en el reconocimiento y viabilidad de las bonificaciones económicas: El monto de la bonificación está delimitado en las directivas; No es posible ofrecer al desmovilizado nada diferente a lo contenido en la misma; cuando se trate de un resultado obtenido por más de un desmovilizado, se expide una sola certificación por la unidad militar y/o de policía y el monto se divide entre quienes brindaron la información; el derecho a la bonificación se causa en el momento en que se encuentran reunidos los requisitos y el viceministro para las políticas y asuntos internacionales firma la orden de pago.

La aplicabilidad en los procedimientos fijados en las directivas ministeriales relacionadas con el tema, admite que cuando se trate del reconocimiento y pago por el aporte eficaz a la administración de justicia o a la fuerza pública entregando información conducente a evitar o esclarecer delitos y/o por la entrega de material de guerra, intendencia, comunicaciones o de cualquier otro elemento que facilite a los grupos armados al margen de la ley el desarrollo de actividades ilícitas, así como de sustancias o drogas estupefacientes, insumos y maquinaria para su elaboración, fabricación y distribución, ocurrida con anterioridad a la vigencia de la presente directiva, se procederá en los términos y condiciones señalados en las directivas permanentes ministeriales números 10 de 2003, 24 de 2004 y 16 de 2007, teniendo en cuenta el estadio temporal en que se obtuvo el resultado operacional.

– Finalmente, el decreto 1059, recientemente aprobado el 4 de abril de 2008, reglamentario de la ley 418 de 1997 y modifica parcialmente los decretos 128 de 2003 y 395 de 2007 en materia de desmovilización individual de los miembros de los grupos de guerrilla que se encuentren privados de la libertad.

El decreto señala que los miembros de los grupos de guerrilla que se encuentren privados de la libertad mediante decisión judicial en cualquier estado de la actuación procesal podrán desmovilizarse de manera individual previa solicitud que elevarán al ministerio del interior y de justicia de conformidad con los formatos que para los efectos se adoptaron a partir del 9 de mayo de 2008 y con el cumplimiento de los requisitos y procedimientos contemplados en el mismo.

El solicitante debe cumplir los siguientes requisitos:

- Haber pertenecido a un grupo de guerrilla con anterioridad a la privación de su libertad e indicar el tiempo de permanencia en el mismo, área de influencia de la respectiva organización guerrillera, actividad que en ella desarrolla y el nombre de los superiores;

- Expresar por escrito su voluntad de abandonar el grupo u organización de guerrilla al cual pertenecía; y

- Colaborar de manera eficaz con las autoridades para el desmantelamiento del grupo de guerrilla del cual forma parte y/o con la administración de justicia para la investigación de las conductas punibles que pudo haber cometido durante su pertenencia el grupo armado organizado al margen de la ley del cual pretende desvincularse.

Recibida la solicitud por el ministerio del interior y de justicia y de encontrarse que se cumple con los requisitos de la solicitud de conformidad con el artículo 3, es remitida a la secretaria técnica del comité operativo para la dejación de las armas, donde se dispone la realización de una entrevista con la finalidad de emitir el ministerio de defensa nacional un concepto técnico sobre la pertenencia del solicitante al grupo de guerrilla del cual pretende desmovilizarse y un concepto valorativo sobre la información y colaboración del solicitante. Una vez se encuentren reunidos la totalidad de documentos pasa cada carpeta al estudio del CODA. De ser certificado obtendrá los beneficios jurídicos por el delito político, apoyo a la familia por la ACR y ubicación en pabellón especial de justicia y paz en caso de someterse a la ley de justicia y paz.

El concepto de pertenencia habilita al núcleo familiar para recibir la ayuda humanitaria del programa de atención humanitaria al desmovilizado, la que se brindará desde el momento que se emita el concepto y hasta cuando determine por el CODA si otorga la certificación o la niega.

Aplicabilidad: Rige a partir de su expedición y se aplica a las personas que con anterioridad a su promulgación (4 DE ABRIL DE 2008), se encontraran privados de la libertad como miembros de grupo de guerrilla.

Finalmente, el anterior contexto constituye las fuentes normativas, en razón al proceso de paz adelantado por el gobierno nacional, observando la imperiosa necesidad de sus reglamentaciones y derogatorias, las cuales influyen en los logros obtenidos dentro de la política de seguridad democrática.

El espacio y el tiempo sobre el cual se realiza la investigación comprenden las unidades tácticas de las fuerzas militares, donde se efectúa la entrevista militar al personal desmovilizado y termina en el grupo de atención humanitaria al

desmovilizado, programa bandera del ministerio de defensa nacional, periodo 2014.

Se hará relación a lo contenido en el código penal militar colombiano[19] Titulo V.

Delitos contra la seguridad de la fuerza pública, capítulo III. De la revelación de secretos, Artículo 130 - Revelación de secretos: El miembro de la fuerza pública que revele documento, acto o asunto concerniente al servicio, con clasificación de seguridad secreto, o ultra secreto, incurrirá en prisión de cinco (5) a ocho (8) años.

Si la revelación fuere de documento, acto o asunto clasificado como reservado, el responsable incurrirá en prisión de dos (2) a cuatro (4) años. Artículo 131.

Revelación Culposa: Si las conductas a que se refiere el artículo anterior se cometieren por culpa, la pena será de uno (1) a dos (2) años de prisión.

2.3 MARCO TECNOLÓGICO

Entendido el por qué la información del desmovilizado debe protegerse pues es una obligación de parte del estado que las fuerzas militares, policía nacional y demás instituciones avaladas por la ley de inteligencia y contrainteligencia que debe garantizar es importante integrar tecnologías que posibiliten tratar, transmitir, procesar, copiar y almacenar esta información.

Pero para poder administrar la información cumpliendo con la confidencialidad, disponibilidad e integridad ante la presencia de múltiples dispositivos para su movilización y almacenamiento, es necesario garantizar que durante el ciclo de vida de la información (creación – procesamiento – almacenamiento, trasmisión y eliminación) no se dejan amenazas, vulnerabilidades y malas prácticas de seguridad sin contemplar[20].

El problema es demasiado grande para una solución definitiva, involucra gente, el eslabón más débil de la cadena de seguridad de la información, tecnologías, aspectos legales, de gestión, y a su vez, que las medidas de precaución no desfavorezcan el uso ágil de la información.

Para garantizar la confidencialidad de la información actualmente se tiene los sistemas Data LossPrevention y para garantizar la privacidad cuando esta se trasmite por una red que no sea de confianza existe la tecnología de capa de

[19] EN COLOMBIA. Código Penal Militar. [En línea]. [Consultado el 24 de enero de 2016]. Disponible en: https://encolombia.com/derecho/codigos/penal-militar/

[20] ESET. (2015). Tendencias 2015: El mundo corporativo en la mira. [En línea]. [Consultado el 24 de enero de 2016]. Disponible en: http://www.welivesecurity.com/wp-content/uploads/2015/01/tendencias_ 2015_eset_mundo_corporativo.pdf

socket segura, SSL - Secure Sockets Layer por sus siglas en inglés y las redes privadas virtuales, VPN – Virtual Private Network por sus siglas en ingles[21].

La tecnología DLP permite Prevenir la revelación intencional o involuntaria de información sensitiva “en reposo”, “en uso” o “en movimiento” hacia partes no autorizadas, y las soluciones VPN permiten comunicarse de manera privada y segura[22].

[21] IBM. Opciones de seguridad en la transmisión. [En línea]. [Consultado el 24 de enero de 2016]. Disponible en: http://www-01.ibm.com/support/knowledgecenter/ssw_ibm_i_71/ rzaj4/rzaj45zh crypto intro.htm?lang=es

[22] SOLÍS, Sergio. Prevención de fuga de datos: Un enfoque para el negocio. [En línea]. [Consultado el 24 de enero de 2016]. Disponible en: http://www.isaca.org/chapters7/ Monterrey/ Events/Documents/20121025%20Preveci%C3%B3n%20de%20Fuga%20de%20Datos.pdf

3. DISEÑO METODOLÓGICO

3.1 HIPÓTESIS DE INVESTIGACIÓN

Hi: Con la metodología para la custodia de las entrevistas militares del personal desmovilizado, desde las unidades tácticas de las fuerzas militares hasta el grupo de atención humanitaria al desmovilizado, se mitigará el riesgo de fuga de información y revelación del secreto, y se fortalecerá la seguridad de la información de la entrevista militar y el prestigio de la institución.

Ho: Con la metodología para la custodia de las entrevistas militares del personal desmovilizado, desde las unidades tácticas de las fuerzas militares hasta el grupo de atención humanitaria al desmovilizado, no se mitigará el riesgo de fuga de información ni la revelación del secreto, ni se fortalecerá la seguridad de la información de la entrevista militar y el prestigio de la institución decaerá al filtrase información reservada para otros fines.

3.2 VARIABLES

3.2.1 Variables Independientes

- Entrevista militar.
- Canal de transmisión.
- Protocolo de seguridad.

3.2.2 Variables Dependientes.

- Riesgo.
- Seguridad de la información.
- Ética de los servidores públicos

3.3 METODOLOGÍA

El presente proyecto se ha enmarcado dentro de la Investigación básica del tipo explicativo, con el cual se busca establecer las causas que generan fuga de información en la entrevista militar practicada a la población desmovilizada, con la ayuda de la tecnología DLP más la información y recomendaciones de expertos en el tema, se establece una metodología para la custodia de las entrevistas militares

del personal desmovilizado, desde las unidades tácticas de las fuerzas militares hasta el grupo de atención humanitaria al desmovilizado.

Se cuenta con algunas variables ya definidas que interactúan en las entrevistas además de personal experto que suministraran por medio de entrevistas, estas variables y el conocimiento del problema de la magnitud de la fuga de información y revelación del secreto, por lo cual se denota la importancia de la presente investigación, teniendo en cuenta que está en juego el prestigio de la institución y del personal que la compone sin dejar de lado la integridad del uno de los actores principales o cliente final que es el Desmovilizado.

4. ESTADO DEL ARTE DEL MANEJO DE LA INFORMACIÓN DE LAS ENTREVISTAS MILITARES DEL PERSONAL DESMOVILIZADO DEL GRUPO DE ATENCIÓN HUMANITARIA AL DESMOVILIZADO

La administración del riesgo para las entidades públicas en todos sus órdenes cobra hoy mayor importancia, dado el dinamismo y los constantes cambios que el mundo globalizado de hoy exige. Estos cambios hacen que dichas entidades deban enfrentarse a factores internos y externos que pueden crear incertidumbre sobre el logro de sus objetivos. Así el efecto que dicha incertidumbre tiene en los objetivos de una organización se denomina "riesgo"[23]

Bajo la sigla SGSI (sistema de gestión de seguridad de la información), se definen procesos sistemáticos, documentados y conocidos por toda la organización, enmarcados en controles específicos estructurados bajo la norma ISO/IEC 27001:2013[24] que permitirán identificar los riesgos a los que está sometida la información y el actuar (asumir, minimizar, transferir o controlar).

ISO 27005 es el estándar internacional que se ocupa de la gestión de riesgos de seguridad de información. La norma suministra las directrices para la gestión de riesgos de seguridad de la información en una empresa, apoyando particularmente los requisitos del sistema de gestión de seguridad de la información definidos en ISO 27001.[25]

Mediante un análisis de brecha se hará la comparación del estado y desempeño real del proceso de entrevista del desmovilizado por parte de los centros de atención al desmovilizado, teniendo como referente la normatividad legal, la metodología de riesgos de la función pública y las normas ISO27001:2013, ISO ISO27005 e ISO31000.

4.1 FASE 1: LEVANTAMIENTO DE INFORMACIÓN

Con el fin de dar cumplimiento a los objetivos planteados en este proyecto se considera necesario hacer el levantamiento de la información que permita identificar, analizar y documentar los elementos que interactúan con la entrevista militar practicada al desmovilizado.

---

[23] INSTITUTO COLOMBIANO DE NORMAS ICONTEC. Norma Técnica Colombiana NTC-ISO31000. [En línea]. [Consultado el 24 de enero de 2016]. Disponible en: http://tienda.icontec.org/brief/NTC-ISO31000.pdf.

[24] INSTITUTO COLOMBIANO DE NORMAS ICONTEC. Norma técnica colombiana ISO/IEC 27002. Tecnologías de Información – Técnicas de Seguridad – Guía de Prácticas de Controles de Seguridad de la Información. 2013. [En línea]. [consultado el 24 de enero de 2016]. Disponible en: www.**iso**27000.es/**iso**27000.html

[25] Ibíd., p. 35

El proceso de desmovilización inicia en la unidad militar donde se presenta la persona que desea integrarse al programa de desmovilizados, las actividades que se realizan en este primer contacto es la realización de una primera entrevista en el formato establecido y catalogado como reservado, la toma de placa dental y entrega de la primera bonificación de vestido; este expediente generado es remitido en formato físico mediante correo certificado o mediante un suboficial de enlace del B2 hacia el GAHD en donde se revisan los documentos enviados y se pasa al departamento de expedientes en donde se hace la verificación del formato físico recibido y se cotejan datos básicos como identificación y posible pertenencia ya al programa. Hechas estas validaciones toda la carpeta es remitida al departamento de desmovilización, al mismo tiempo que en el hogar de paz se realiza la segunda entrevista al personal, entrevista que es enviada digitalmente mediante correo de internet. Esta segunda entrevista realizada en el hogar de paz junto con la primera realizada en la unidad militar es confrontada para verificar que no existan inconsistencias ni falsedad de información para poder emitir el concepto de voluntad y pertenencia; concepto que es entregado nuevamente al departamento de expediente quien hace una revisión y validación antes de entregar al CODA (comité operativo dejación armas) quien en definitiva es quien toma la decisión de aprobado – aplazado o negado; si la decisión es aplazado se toman 8 días adicionales para la solicitud de más información a entidades del estado; si la decisión es aceptado o negado el expediente se digitaliza se sube al repositorio y el físico va a resguardo con la empresa MTI con quien se tiene contrato.

En este proceso participan 3 dependencias Archivo, expedientes y CODA por los cuales el formato de entrevista se mueve como activo de información, fue necesario realizar auditoria a estas 3 dependencias para analizar el proceso de entrevista del desmovilizado con base en la ley 1581 de 2012 protección de datos personales (ver anexo A), ley 1621 de 2013 (ver anexo B) y decreto 857 de 14 (ver anexo C).

En esta auditoría se verifico (Ver anexo F – G)

- Las actas diligenciadas de confidencialidad de información de los funcionarios; según lo mandado en el artículo 38 de la ley 1621 del 17 de abril del 2013 las cuales deben conservarse aun después del cese de sus funciones[26] y deben demostrar que el personal cumple y cumplió en todo momento los más altos estándares de idoneidad y confianza que permitan mantener el compromiso de reserva en el desarrollo de sus funciones[27] (ver anexo B)

[26] PRESIDENCIA DE COLOMBIA. Ley de Inteligencia y Contra Inteligencia. Ley 1621 del 17 de abril de 2013 - Articulo 38 – Párrafo 1. [en línea]. [Consultado el 24 de enero 2016]. Disponible en: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/2013/LEY%201621%20DEL%2017%20DE%20ABRIL%20DE%202013.pdf

[27] Ibíd.

- Credenciales de autorización de manejo de información reservada de acuerdo a su función; definidos en el artículo 36 y 37 de la ley 1621 del 17 de abril del 2013[28] (ver anexo B)

- Repositorios autorizados de información, definidos en el capítulo V artículos 28 y 29 de la ley 1621 del 17 de abril del 2013[29] (ver anexo B)

- Clasificación de documentos de acuerdo al artículo 11 del decreto 857/201430 (ver anexo C).

- Uso de dispositivos electrónicos personales al interior del GAHD
- Manejo de documentos físicos en los escritorios

Con esta información recolectada se realizará la identificación de riesgos, análisis de riesgos, valoración de riesgos para el proceso de entrevistas del personal desmovilizado del GAHD.

4.2 FASE 2: IDENTIFICACIÓN, ANÁLISIS Y VALORACIÓN DEL RIESGO FRENTE A LA INFORMACIÓN

El cumplimiento de objetivos de las entidades de administración pública puede verse afectado por factores internos y externos que generan riesgos frente a sus actividades, razón por la cual se hace necesario contar con acciones tendientes a administrarlos

De acuerdo a la norma Técnica NTC-ISO31000 se interpreta que la eficacia del control está en el manejo de los riesgos, es por eso que se realizara el análisis y valoración del riesgo frente a la información teniendo en cuenta su criticidad frente a la integridad, disponibilidad y confidencialidad con el fin de reducir o mitigar su ocurrencia.

Este análisis se concentra en los riesgos operativos que son los que comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.

La valoración de activos de información frente a la seguridad que se aplicó se enmarco en la disponibilidad, integridad y confidencialidad.

---

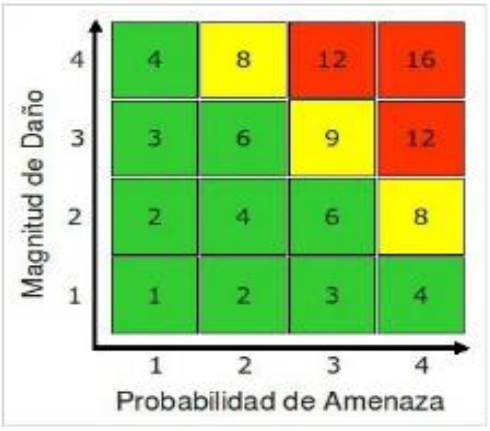
[28] Ibíd.
[29] Ibíd.
[30] PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA. Decreto 857 de 2104 – Articulo 11. [En línea]. [Consultado el 16 de enero de 2016]. Disponible en http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201712%20DEL%2006%20DE%20MARZO%20DE%2014.pdf

La matriz de riesgo a aplicar se basará en la formula Riesgo = Probabilidad de Amenaza x Magnitud de daño, de acuerdo a la figura 2.

La probabilidad de amenaza y magnitud de daño pueden tomar los valores de condición respectivamente

- 1 = Insuficiente (Incluida ninguna)
- 2 = Baja
- 3 = Mediana
- 4 = Alta

Figura 2. Magnitud daño vs probabilidad de amenaza



Fuente: autores

El riesgo producto de la multiplicación esta agrupado en 3 rangos

- Bajo Riesgo = 1 – 6 (Verde)
- Medio Riesgo = 8 – 9 (Amarillo)
- Alto Riesgo = 12 – 16 (Rojo)

Los activos de información que se analizaron para obtener la valoración del riesgo son – Ver anexo H – I – J – Matriz de análisis de riesgo

- El formato de Informe de Entrevista del desmovilizado (Entiéndase como el archivo físico/digital con información suministrada en la entrevista) (ver anexo E).

- El equipo de cómputo con el que se realiza la entrevista

- El personal/funcionario que realiza la entrevista

Dependiendo de los valores de la probabilidad de amenaza y la magnitud de daño, la matriz calcula el producto de ambas variables y visualiza el grado de riesgo

Cuadro 1. Análisis de riesgo promedio

		Probabilidad de Amenaza		
		Confidencialidad	Integridad	Disponibilidad
Magnitud de Daño	Datos e Información	16,0	12,0	12,0
	Sistemas e Infraestructura	12,0	10,5	9,0
	Personal	10,0	16,0	10,0

Fuente: autores

Dependiendo del color de cada celda del cuadro 1, se puede concluir que:

- El formato de informe de entrevista tiene un alto riesgo de sufrir amenazas con respecto a la confidencialidad (fuga de información, accesos no autorizados al formato digital), integridad (alteración/modificación de las preguntas) y disponibilidad (destrucción y plagio).

- El equipo de cómputo con el que se realizan las entrevistas en los hogares de paz y en las unidades militares tiene un Alto riesgo de sufrir amenazas con respecto a la confidencialidad (accesos a dispositivos externos, uso de equipos de terceros o externos) y un riesgo medio de sufrí amenazas con respecto a la Integridad (uso de software no licenciado, no uso de software antivirus/antispyware) y disponibilidad (rutinas de mantenimiento preventivo y correctivo, retiro e ingreso de equipos de la institución).

- El personal/funcionario público/entrevistador tiene un alto riesgo de sufrir amenazas con relación a la integridad (suplantación/reemplazos no autorizados, amenaza/soborno/influencia externa) y un riesgo medio de sufrir amenazas con respecto a la confidencialidad (cumplimiento artículos 36 – 37 y 38 ley 1621/2013) (ver anexo B), y disponibilidad (ausencia de Personal capacitado para la toma de entrevista, no existencia de unidad Militar para presentación de desmovilizados y toma de entrevista).

Para facilitar la calificación y evaluación del riesgo se usa una matriz cualitativa que permite responder a los riesgos, esta matriz es la que se observa en la cuadro 2.

Cuadro 2. Matriz calificación y evaluación del riesgo

Probabilidad	IMPACTO			
	Insignificante (1)	Bajo (2)	Medio (3)	Alto (4)
Insignificante (1)	B	B	M	M
Bajo (2)	B	B	M	M
Medio (3)	B	M	A	E
Alto (4)	M	A	A	E

Fuente: autores

B: Zona de riesgo baja: Asumir el riesgo
M: Zona de riesgo moderada: Asumir el riesgo, reducir el riesgo
A: Zona de riesgo Alta: Reducir el riesgo, evitar, compartir o transferir
E: Zona de riesgo extrema: Reducir el riesgo, evitar, compartir o transferir

Para cada activo de información se hace el análisis del riesgo actual (ver cuadro 3 – 4 – 5), el cual será el punto de partida.

Cuadro 3. Análisis del riesgo - activo formato entrevista

ANÁLISIS DEL RIESGO				
Activo: Formato Entrevista				
Clasificación: Confidencial – Privado – Obligación por ley				
RIESGO	CALIFICACIÓN		Evaluación	Medida de Respuesta
	Probabilidad	Impacto		
Confidencialidad – Fuga de Información	4	4	E	Reducir, evitar, compartir, transferir
Confidencialidad - Acceso no autorizado al formato del sistema	4	4	E	Reducir, evitar, compartir, transferir
Integridad - Alteración/modificación Preguntas	3	4	E	Reducir, evitar, compartir, transferir
Modificación Información Diligenciada o ya ingresada	3	4	E	Reducir, evitar, compartir, transferir
Disponibilidad – Destrucción	3	4	E	Reducir, evitar, compartir, transferir
Disponibilidad – Plagio	3	4	E	Reducir, evitar, compartir, transferir

Fuente: autores

Cuadro 4. Análisis del riesgo - activo equipo de cómputo para entrevista

ANÁLISIS DEL RIESGO				
Activo: Equipo de cómputo para Entrevista				
Clasificación: Acceso Exclusivo				
RIESGO	CALIFICACIÓN		Evaluación	Medida de Respuesta
	Probabilidad	Impacto		
Confidencialidad – Acceso a dispositivos Externos	4	3	E	Reducir, evitar, compartir, transferir
Confidencialidad - Uso de equipos externos/personales	4	3	E	Reducir, evitar, compartir, transferir
Integridad - Uso de software no licenciado	4	3	E	Reducir, evitar, compartir, transferir
Integridad - No uso de software antivirus/antispyware	3	3	A	Reducir, evitar, compartir, transferir
Disponibilidad – No realización de Mantenimiento preventivo/correctivo	3	3	A	Reducir, evitar, compartir, transferir
Disponibilidad – Retiro e ingreso de equipos de la institución	3	3	A	Reducir, evitar, compartir, transferir

Fuente: autores

Cuadro 5. Análisis del riesgo - activo entrevistador

ANÁLISIS DEL RIESGO				
Activo: Entrevistador				
Clasificación: Perfil Medio – experto en su área				
RIESGO	CALIFICACIÓN		Evaluación	Medida de Respuesta
	Probabilidad	Impacto		
Confidencialidad – No Existencia de actas de confidencialidad - Art38 Ley1621/2013	3	4	E	Reducir, evitar, compartir, transferir
Confidencialidad - Error en la asignación de Credenciales y Roles – Art36 - 37 Ley 1621/2013 (ver anexo B)	2	4	M	Reducir, Asumir
Integridad - Suplantación/Reemplazo no autorizado	4	4	E	Reducir, evitar, compartir, transferir
Integridad – Amenaza/soborno/influencia externa	4	4	E	Reducir, evitar, compartir, transferir
Disponibilidad – Ausencia de Personal capacitado para la toma de entrevista	4	4	E	Reducir, evitar, compartir, transferir
Disponibilidad – No existencia de Unidad Militar para presentación de desmovilizados y toma de entrevista	1	4	M	Reducir, Asumir

Fuente: autores

Este primer análisis del riesgo se denomina Riesgo Inherente[31] y se define como aquél al que se enfrenta una entidad en ausencia de acciones por parte de la dirección para modificar su probabilidad o impacto.

La valoración del riesgo resulta de confrontar los resultados de la evaluación del riesgo con los controles identificados, para poder establecer prioridades en su manejo y en la fijación de la política.

Para realizar la valoración de los controles existentes es necesario recordar que estos se clasifican en[32]:

– Preventivos: aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurrencia.

[31] INCODER Administración de Riesgos Corporativos. Técnicas de Aplicación Colombia. USA; Price Waterhouse Coopers, 2005. p. 39

[32] MINISTERIO DEL TRABAJO Y SEGURIDAD SOCIAL. Guía para la administración del riesgo – DAFP [En línea]. [Consultado el 29 de enero de 2016]. Disponible en: http://portal.dafp.gov.co/portal/pls/portal/formularios.retrive_publicaciones?no=1592

– Correctivos: aquellos que permiten el restablecimiento de la actividad, después de ser detectado un evento no deseable; también la modificación de las acciones que propiciaron su ocurrencia.

Actualmente existen normativas, y tecnologías que ayudarían a minimizar ese riesgo inherente; los controles a nivel de normativa no están siendo de estricto cumplimiento para el proceso de la entrevista al desmovilizado y a nivel de tecnologías no están implementadas como deben ser.

En el cuadro 6, se presenta un listado de controles existentes:

Cuadro 6. Listado controles existentes

Control	Tipo	Cubre	Clasificación
Ley 1712 de 2014 – Ley de transparencia y del Derecho de Acceso a la Información Pública Nacional. Reglamenta la necesidad de contar con información confiable y oportuna, fortalecer los esquemas de publicación de información, crear y mantener actualizado el registro de activos de información para uso y disposición del público. – Artículo 15 – Programa de gestión documental. (Ver anexo D).	Normativo	Probabilidad	Preventivo
Ley 1621 de 2013 – Ley de inteligencia y contrainteligencia – Articulo 28 (ver anexo B) y Articulo 15 Decreto 857 de 2014 – Centros de protección de datos de inteligencia y contra inteligencia.	Normativo	Probabilidad	Preventivo
Ley 1621 de 2013 – Ley de inteligencia y contrainteligencia – Articulo 38 Compromiso de Reserva(ver anexo B)	Normativo	Probabilidad	Preventivo
Decreto 857 de 2014 – Reglamenta Ley 1621 de 2013 - Articulo 20 – Estudios de credibilidad y confiabilidad. (ver anexo B)	Normativo	Probabilidad	Preventivo
política de seguridad MDN - DIR2014-18 del 19 de junio de 2014,	Normativo	Probabilidad	Preventivo
Time Stamping – Sellado de tiempo - es un mecanismo en línea que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo[33]	Tecnológico	Probabilidad	Preventivo

Fuente: autores

[33] IZENPE. Sellado de Tiempo. [En línea]. [Consultado el 29 de enero de 2016]. Disponible en www.izenpe.com/s15.../es/...sellado_tiempo/es.../servicios_de_sellado _tiempo.html

Cuadro 6. Listado controles existentes (continuación)

Control	Tipo	Cubre	Clasificación
Función hash – Firma Digital - Una función hash es un método para generar claves o llaves que representen de manera casi unívoca a un documento o conjunto de datos. Es una operación matemática que se realiza sobre este conjunto de datos de cualquier longitud, y su salida es una huella digital, de tamaño fijo e independiente de la dimensión del documento original.[34]	Tecnológico	Probabilidad	Preventivo
La tecnología DLP permite Prevenir la revelación intencional o involuntaria de información sensitiva "en reposo", "en uso" o "en movimiento" hacia partes no autorizadas[35],	Tecnológico	Probabilidad	Preventivo
Soluciones VPN permiten comunicarse de manera privada y segura.	Tecnológico	Probabilidad	Preventivo

Fuente: autores

Y se usa el cuadro 7 para un análisis de tipo cuantitativo, el cual indicara con exactitud cuántas posiciones dentro de la matriz de calificación, evaluación y respuesta a los riesgos es posible desplazarse (ver cuadro 9)

Cuadro 7. Matriz calificación y evaluación del riesgo

Probabilidad	IMPACTO			
	Insignificante (1)	Bajo (2)	Medio (3)	Alto (4)
Insignificante (1)	B	B	M	M
Bajo (2)	B	B	M	M
Medio (3)	B	M	A	E
Alto (4)	M	A	A	E

Fuente: autores

B: Zona de riesgo baja: Asumir el riesgo
M: Zona de riesgo moderada: Asumir el riesgo, reducir el riesgo
A: Zona de riesgo Alta: Reducir el riesgo, evitar, compartir o transferir
E: Zona de riesgo extrema: Reducir el riesgo, evitar, compartir o transferir

[34] CERT. Hashing. [En línea]. [Consultado el 29 de enero de 2016]. Disponible en www.cert.fnmt.es/content/pages_std/html/tutoriales/tuto7.htm
[35] SOLÍS Sergio. Prevención de fuga de datos - Un enfoque para el negocio. [En línea]. [Consultado el 24 de enero del 2016]. Disponible en http://www.isaca.org/chapters7/Monterrey/Events/Documents/20121025%20Preveci%C3%B3n%20de%20Fuga%20de%20Datos.pdf

También es necesario definir unos criterios con los cuales se va a medir la aplicabilidad de los controles (ver cuadro 8)

Cuadro 8. Criterios aplicabilidad controles

PARÁMETROS	CRITERIOS	TIPO DE CONTROL		PUNTAJES
		Probabilidad	Impacto	
Herramientas para ejercer el control	Posee una herramienta para ejercer el control o Existen manuales instructivos o procedimientos para el manejo de la herramienta			30
	En el tiempo que lleva la herramienta ha demostrado ser efectiva			30
Seguimiento al control	Están definidos los responsables de la ejecución del control y del seguimiento.			15
	La frecuencia de la ejecución del control y seguimiento es adecuada			25
TOTAL				100

Fuente: autores

Ya con esto se entra a valorar los controles, para lo cual se necesita ponderar de manera objetiva y así poder determinar el desplazamiento dentro de la matriz de clasificación (ver cuadro 9).

Cuadro 9. Desplazo matriz de calificación, evaluación y respuesta a los riesgos

RANGOS DE CALIFICACIÓN DE LOS CONTROLES	DEPENDIENDO SI EL CONTROL AFECTA PROBABILIDAD O IMPACTO DESPLAZA EN LA MATRIZ DE CALIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS	
	CUADRANTES A DISMINUIR EN LA PROBABILIDAD	CUADRANTES A DISMINUIR EN EL IMPACTO
Entre 0-30	0	0
Entre 11-54	1	1
Entre 55-100	2	2

Fuente: autores

Para realizar la valoración del riesgo de los activos de información estudiados se usó para el activo formato informe de entrevista los cuadros del 10 al 15, para el activo Equipo de cómputo entrevista los cuadros del 17 al 22 y para el activo funcionario público / entrevistador los cuadros del 24 al 29.

El resultado obtenido a través de la valoración del riesgo (ver cuadros 17, 23 y 30) es denominado también tratamiento del riesgo, ya que se “involucra la selección de una o más opciones para modificar los riesgos y la implementación de tales

acciones"[36], así el desplazamiento dentro de la matriz de evaluación y calificación determinará finalmente la selección de las opciones de tratamiento del riesgo, así[37]:

- Evitar el riesgo, tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas.

- Reducir el riesgo, implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles.

- Compartir o transferir el riesgo, reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido.

- Asumir un riesgo, luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso, el gerente del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

Para lograr modificar el riesgo y llegar a cualquiera de las posiciones del tratamiento del riesgo es necesario la elaboración de un plan encaminado al rediseño de controles existente, diseño de nuevos controles, supresión de controles redundantes, mejora en la implementación de controles o mejora en la efectividad de los controles.

Para lograr la custodia de las entrevistas militares del personal desmovilizado este plan se debe basar en el re-diseño de nuevos controles, mejora en la implementación de controles y la medición de la efectividad de controles.

Veamos cómo sería el proceso de entrevista durante todo su ciclo de vida con la implementación de controles:

Todo el proceso esta cobijado bajo el control normativo de la ley 1621 del 2013 en su artículo 33; como es una actividad de una entidad que lleva a cabo funciones de inteligencia y contra inteligencia la información es considerada de reserva legal (ver anexo B).

[36]NORMA TÉCNICA COLOMBIANA. Op. Cit. p. 30
[37] MINISTERIO DEL TRABAJO Y SEGURIDAD SOCIAL. Op. Cit. p. 43

Al momento de la presentación del ciudadano con la intención de desmovilizarse este también esta cobijado por la normatividad y obligado a ejecutar la actividad con la verdad y sin influir ni inducir al entrevistador de acuerdo al artículo 453 del código penal – fraude procesal.

El funcionario de las fuerzas militares también está bajo la normativa del artículo 38 – Compromiso de reserva - de la ley de inteligencia y contra inteligencia ley 1621 de 2013 (ver anexo B) y del artículo 20 – Estudios de credibilidad y confiabilidad – decreto 857 de 2014.

El equipo de cómputo desde el que se realizara la entrevista está bajo los controles definidos en la política de seguridad del MDN – reglamentados en la directiva DIR2014-18 del 19 de junio del 2014.

El formato de informe de entrevista – archivo digitalizado donde se consigna la información producto de la entrevista debe esta resguardado en un repositorio único de acuerdo a lo descrito en el artículo 28 de la ley 1621 del 2013 (ver anexo B) y del artículo 15 del decreto 857 del 2014.

El acceso al repositorio de almacenamiento está controlado mediante registro y validación de usuario, de acuerdo a lo establecido en la política de seguridad del MDN reglamentados en la directiva DIR2014-18 del 19 de junio del 2014.

El servicio de acceso al formato esta dado de acuerdo a las reglas registradas en el software DLP.

Una vez diligenciada la entrevista se aplica el control de estampa de tiempo (Time stamping), para garantizar que a partir de ese momento el archivo existe y que no será modificado.

Dependiendo de la forma como se reportará la actividad de la entrevista se decide si el documento se imprime o se envía digital; si se requiere impresión de acuerdo a las reglas del sistema DLP y a la política de seguridad del MDN el equipo tendrá acceso a una impresora posterior teniendo el documento en físico por su carácter de Reservado se realiza el oficio remisorio y custodia hasta su entrega

Si se requiere él envió digital como es el caso de los hogares de paz, mediante la combinación de los controles de función hash – firma digital, reglas del sistema DLP y establecimiento de canal seguro mediante el sistema VPN se envía la información.

El proceso de recepción y consulta desde cualquier otra dependencia sigue estando bajo los controles y características de la política de seguridad del MDN, las reglas de control de información del DLP y la condición de reserva legal de la ley 1621 del 2013 (ver anexo B).

Cuadro 10. Valoración del riesgo - formato informe entrevista - fuga información

VALORACIÓN DEL RIESGO							
Activo: Formato Informe Entrevista							
RIESGO	CALIFICACIÓN		CONTROLES	VALORACIÓN			
	Probabilidad	Impacto		Tipo Control Probabilidad O Impacto.	PUNTAJE Herramientas para ejercer el control	PUNTAJE Seguimiento al control	Puntaje Final
Fuga de Información	4	4	Sistema DLP con reglas de control de flujo y control de información	Probabilidad	30	25	55
				Desplaza 2 casillas de probabilidad			

Fuente: autores

Cuadro 11. Valoración del riesgo - formato informe entrevista - acceso no autorizado al formato del sistema

VALORACIÓN DEL RIESGO							
Activo: Formato Informe Entrevista							
RIESGO	CALIFICACIÓN		CONTROLES	VALORACIÓN			
	Probabilidad	Impacto		Tipo Control Probabilidad O Impacto	PUNTAJE Herramientas para ejercer el control	PUNTAJE Seguimiento al control	Puntaje Final
Acceso no autorizado al formato del sistema	4	4	Repositorio Único de información con permisos y roles asignados	Probabilidad.	30	25	55
				Desplaza 2 casillas de probabilidad			

Fuente: autores

Cuadro 12. Valoración del riesgo - formato informe entrevista - alteración/modificación preguntas

VALORACIÓN DEL RIESGO							
Activo: Formato Informe Entrevista							
RIESGO	CALIFICACIÓN		CONTROLES	VALORACIÓN			
	Probabilidad	Impacto		Tipo Control Probabilidad O Impacto	PUNTAJE Herramientas para ejercer el control	PUNTAJE Seguimiento al control	Puntaje Final
Alteración/modificación Preguntas	3	4	Repositorio Único de información con permisos y roles asignados	Probabilidad	30	25	55
				Desplaza 2 casillas de probabilidad			

Fuente: autores

Cuadro 13. Valoración del riesgo - formato informe entrevista - modificación información diligenciada ya ingresada

VALORACIÓN DEL RIESGO							
Activo: Formato Informe Entrevista							
RIESGO	CALIFICACIÓN		CONTROLES	VALORACIÓN			
	Probabilidad	Impacto		Tipo Control Probabilidad O Impacto	PUNTAJE Herramientas para ejercer el control	PUNTAJE Seguimiento al control	Puntaje Final
Modificación Información Diligenciada o ya ingresada	3	4	Repositorio Único de información con permisos y roles asignados	Probabilidad	30	25	55
				Desplaza 2 casillas de probabilidad			

Fuente: autores

Cuadro 14. Valoración del riesgo - formato informe entrevista - destrucción

VALORACIÓN DEL RIESGO							
Activo: Formato Informe Entrevista							
RIESGO	CALIFICACIÓN		CONTROLES	VALORACIÓN			
	Probabilidad	Impacto		Tipo Control Probabilidad O Impacto	PUNTAJE Herramientas para ejercer el control	PUNTAJE Seguimiento al control	Puntaje Final
Destrucción	3	4	Repositorio Único de información con permisos y roles asignados	Probabilidad	30	25	55
				Desplaza 2 casillas de probabilidad			

Fuente: autores

Cuadro 15. Valoración del riesgo - formato informe entrevista - plagio

VALORACIÓN DEL RIESGO							
Activo: Formato Informe Entrevista							
RIESGO	CALIFICACIÓN		CONTROLES	VALORACIÓN			
	Probabilidad	Impacto		Tipo Control Probabilidad O Impacto	PUNTAJE Herramientas para ejercer el control	PUNTAJE Seguimiento al control	Puntaje Final
Plagio	3	4	Repositorio Único de información con permisos y roles asignados	Probabilidad	30	25	55
				Desplaza 2 casillas de probabilidad			

Fuente: autores

Cuadro 16. Mapa de riesgos - activo formato informe entrevista

MAPA DE RIESGOS									
Activo: Formato Informe Entrevista									
Riesgo	Calificación		Evaluación Riesgo	Controles	Nueva Calificación		Nueva Evaluación	Opciones de Manejo	Acciones
	Probabilidad	Impacto			Probabilidad	Impacto			
Fuga de Información	4	4	E= zona de Riesgo Extrema	Sistema DLP con reglas de control de flujo y control de información Y VPN para comunicación segura	2	4	M= zona de riesgo moderada	Asumir, Reducir	Endurecer políticas DLP y configurar VPN
Acceso no autorizado al formato del sistema	4	4	E= zona de Riesgo Extrema	Repositorio Único de información con permisos y roles asignados	2	4	M= zona de riesgo moderada	Asumir, Reducir	Creación de repositorio único de información
Alteración/modificación preguntas	3	4	E= zona de Riesgo Extrema	Repositorio Único de información con permisos y roles asignados	1	4	M= zona de riesgo moderada	Asumir, Reducir	Creación de repositorio único de información
Modificación Información Diligenciada o ya ingresada	3	4	E= zona de Riesgo Extrema	Repositorio Único de información con permisos y roles asignados	1	4	M= zona de riesgo moderada	Asumir, Reducir	Creación de repositorio único de información
Destrucción	3	4	E= zona de Riesgo Extrema	Repositorio Único de información con permisos y roles asignados	1	4	M= zona de riesgo moderada	Asumir, Reducir	Creación de repositorio único de información
Plagio	3	4	E= zona de Riesgo Extrema	Repositorio Único de información con permisos y roles asignados	1	4	M= zona de riesgo moderada	Asumir, Reducir	Creación de repositorio único de información

Fuente: autores

Cuadro 17. Valoración del riesgo - activo equipo de cómputo entrevista - acceso a dispositivos externos

VALORACIÓN DEL RIESGO							
Activo: Equipo de Entrevista							
RIESGO	CALIFICACIÓN		CONTROLES	VALORACIÓN			
	Probabilidad	Impacto		Tipo Control Probabilidad O Impacto	PUNTAJE Herramientas para ejercer el control	PUNTAJE Seguimiento al control	Puntaje Final
Acceso a dispositivos Externos	4	3	Aplicación de Política de seguridad MDN	Probabilidad	30	25	55
				Desplaza 2 casillas de probabilidad			

Fuente: autores

Cuadro 18. Valoración del riesgo - activo equipo de cómputo entrevista - uso de equipos externos/personales

VALORACIÓN DEL RIESGO							
Activo: Equipo de Entrevista							
RIESGO	CALIFICACIÓN		CONTROLES	VALORACIÓN			
	Probabilidad	Impacto		Tipo Control Probabilidad O Impacto	PUNTAJE Herramientas para ejercer el control	PUNTAJE Seguimiento al control	Puntaje Final
Uso de equipos externos/personales	4	3	Aplicación de Política de seguridad MDN	Probabilidad	30	25	55
				Desplaza 2 casillas de probabilidad			

Fuente: autores

Cuadro 19. Valoración del riesgo - activo equipo de cómputo entrevista - uso de software no licenciado

VALORACIÓN DEL RIESGO							
Activo: Equipo de Entrevista							
RIESGO	CALIFICACIÓN		CONTROLES	VALORACIÓN			
	Probabilidad	Impacto		Tipo Control Probabilidad O Impacto	PUNTAJE Herramientas para ejercer el control	PUNTAJE Seguimiento al control	Puntaje Final
Uso de software no licenciado	4	3	Aplicación de Política de seguridad MDN	Probabilidad	30	25	55
				Desplaza 2 casillas de probabilidad			

Fuente: autores

Cuadro 20. Valoración del riesgo - activo equipo de cómputo entrevista - no uso de software antivirus/antispyware

VALORACIÓN DEL RIESGO							
Activo: Equipo de Entrevista							
RIESGO	CALIFICACIÓN		CONTROLES	VALORACIÓN			
	Probabilidad	Impacto		Tipo Control Probabilidad O Impacto	PUNTAJE Herramientas para ejercer el control	PUNTAJE Seguimiento al control	Puntaje Final
No uso de software antivirus/antispyware	3	3	Aplicación de Política de seguridad MDN	Probabilidad	30	25	55
				Desplaza 2 casillas de probabilidad			

Fuente: autores

Cuadro 21. Valoración del Riesgo - activo equipo de cómputo entrevista - no realización de mantenimiento

VALORACIÓN DEL RIESGO							
Activo: Equipo de Entrevista							
RIESGO	CALIFICACIÓN		CONTROLES	VALORACIÓN			
	Probabilidad	Impacto		Tipo Control Probabilidad O Impacto	PUNTAJE Herramientas para ejercer el control	PUNTAJE Seguimiento al control	Puntaje Final
No realización de Mantenimiento preventivo/correctivo	3	3	Aplicación de Política de seguridad MDN	Probabilidad	30	25	55
				Desplaza 2 casillas de probabilidad			

Fuente: autores

Cuadro 22. Valoración del riesgo - activo equipo de cómputo entrevista - retiro e ingreso de equipos de la institución

VALORACIÓN DEL RIESGO							
Activo: Equipo de Entrevista							
RIESGO	CALIFICACIÓN		CONTROLES	VALORACIÓN			
	Probabilidad	Impacto		Tipo Control Probabilidad O Impacto	PUNTAJE Herramientas para ejercer el control	PUNTAJE Seguimiento al control	Puntaje Final
Retiro e ingreso de equipos de la institución	3	3	Aplicación de Política de seguridad MDN	Probabilidad	30	25	55
				Desplaza 2 casillas de probabilidad			

Fuente: autores

Cuadro 23. Mapa de riesgos - activo equipo de cómputo entrevistas

MAPA DE RIESGOS									
Activo: Equipo cómputo para hacer entrevistas									
Riesgo	Calificación		Evaluación Riesgo	Controles	Nueva Calificación		Nueva Evaluación	Opciones de Manejo	Acciones
	Probabilidad	Impacto			Probabilidad	Impacto			
Acceso a dispositivos Externos	4	3	A= zona de Riesgo Alta	Implementación política de Seguridad del MDN	2	3	M= zona de riesgo moderada	Asumir, Reducir	Socialización y capacitación de la política
Uso de equipos externos/personales	4	3	A= zona de Riesgo Alta	Implementación política de Seguridad del MDN	2	3	M= zona de riesgo moderada	Asumir, Reducir	Socialización y capacitación de la política
Uso de software no licenciado	4	3	A= zona de Riesgo Alta	Implementación política de Seguridad del MDN	2	3	M= zona de riesgo moderada	Asumir, Reducir	Socialización y capacitación de la política
No uso de software antivirus/antispyware	3	3	A= zona de Riesgo Alta	Implementación política de Seguridad del MDN	1	3	M= zona de riesgo moderada	Asumir, Reducir	Socialización y capacitación de la política
No realización de Mantenimiento preventivo/correctivo	3	3	A= zona de Riesgo Alta	Implementación política de Seguridad del MDN	1	3	M= zona de riesgo moderada	Asumir, Reducir	Socialización y capacitación de la política
Retiro e ingreso de equipos de la institución	3	3	A= zona de Riesgo Alta	Implementación política de Seguridad del MDN	1	3	M= zona de riesgo moderada	Asumir, Reducir	Socialización y capacitación de la política

Fuente: autores

Cuadro 24. Valoración del riesgo - activo funcionario público/entrevistador - no existencia de actas

VALORACIÓN DEL RIESGO							
Activo: Funcionario Público Entrevistador							
RIESGO	CALIFICACIÓN		CONTROLES	VALORACIÓN			
	Probabilidad	Impacto		Tipo Control Probabilidad O Impacto	PUNTAJE Herramientas para ejercer el control	PUNTAJE Seguimiento al control	Puntaje Final
No Existencia de actas de confidencialidad - Art38 Ley1621/2013(ver anexo B)	3	4	Cumplimiento Art. 38	Probabilidad	30	25	55
				Desplaza 2 casillas de probabilidad			

Fuente: autores

Cuadro 25. Valoración del riesgo - activo funcionario público/entrevistador - error en asignación de credenciales

VALORACIÓN DEL RIESGO							
Activo: Funcionario Público Entrevistador							
RIESGO	CALIFICACIÓN		CONTROLES	VALORACIÓN			
	Probabilidad	Impacto		Tipo Control Probabilidad O Impacto	PUNTAJE Herramientas para ejercer el control	PUNTAJE Seguimiento al control	Puntaje Final
Error en la asignación de Credenciales y Roles – Art36 - 37 Ley 1621/2013(ver anexo B)	2	4	Cumplimiento Art. 36	Probabilidad	30	15	45
				Desplaza 1 casillas de probabilidad			

Fuente: autores

Cuadro 26. Valoración del riesgo - activo funcionario público/entrevistador - suplantación/reemplazo no autorizado

VALORACIÓN DEL RIESGO							
Activo: Funcionario Público Entrevistador							
RIESGO	CALIFICACIÓN		CONTROLES	VALORACIÓN			
	Probabilidad	Impacto		Tipo Control Probabilidad O Impacto	PUNTAJE Herramientas para ejercer el control	PUNTAJE Seguimiento al control	Puntaje Final
Suplantación/Reemplazo no autorizado	4	4	Cumplimiento Art. 38	Probabilidad	30	25	55
				Desplaza 2 casillas de probabilidad			

Fuente: autores

Cuadro 27. Valoración del riesgo - activo funcionario público/entrevistador - amenaza/soborno/influencia externa

VALORACIÓN DEL RIESGO							
Activo: Funcionario Público Entrevistador							
RIESGO	CALIFICACIÓN		CONTROLES	VALORACIÓN			
	Probabilidad	Impacto		Tipo Control Probabilidad O Impacto	PUNTAJE Herramientas para ejercer el control	PUNTAJE Seguimiento al control	Puntaje Final
Amenaza/soborno/influencia externa	4	4	Cumplimiento Art. 38	Probabilidad	30	25	55
				Desplaza 2 casillas de probabilidad			

Fuente: autores

Cuadro 28. Valoración del riesgo - activo funcionario público/entrevistador - ausencia de personal capacitado

VALORACIÓN DEL RIESGO							
Activo: Funcionario Público Entrevistador							
RIESGO	CALIFICACIÓN		CONTROLES	VALORACIÓN			
	Probabilidad	Impacto		Tipo Control Probabilidad O Impacto	PUNTAJE Herramientas para ejercer el control	PUNTAJE Seguimiento al control	Puntaje Final
Ausencia de Personal capacitado para la toma de entrevista	4	4	Cumplimiento Art. 38	Probabilidad	30	25	55
				Desplaza 2 casillas de probabilidad			

Fuente: autores

Cuadro 29. Valoración del riesgo - activo funcionario público/entrevistador - no existencia de unidad militar

VALORACIÓN DEL RIESGO							
Activo: Funcionario Público Entrevistador							
RIESGO	CALIFICACIÓN		CONTROLES	VALORACIÓN			
	Probabilidad	Impacto		Tipo Control Probabilidad O Impacto	PUNTAJE Herramientas para ejercer el control	PUNTAJE Seguimiento al control	Puntaje Final
No existencia de Unidad Militar para presentación de desmovilizados y toma de entrevista	1	4	Cumplimiento Decreto 857/2014	Probabilidad	30	0	30
				Desplaza 0 casillas de probabilidad			

Fuente: autores

Cuadro 30. Mapa de riesgos - activo funcionario público/entrevistador

MAPA DE RIESGOS									
Activo: Funcionario Público / Entrevistador									
Riesgo	Calificación		Evaluación Riesgo	Controles	Nueva Calificación		Nueva Evaluación	Opciones de Manejo	Acciones
	Probabilidad	Impacto			Probabilidad	Impacto			
No Existencia de actas de confidencialidad - Art38 Ley1621/2013	3	4	A= zona de Riesgo Alta	Cumplimiento Art. 38	1	4	M= zona de riesgo moderada	Asumir, Reducir	Control Interno cumplimiento de la ley
Error en la asignación de Credenciales y Roles - Art36 - 37 Ley 1621/2013 (ver anexo B)	2	4	M= zona de riesgo moderada	Cumplimiento Art. 36-37	1	4	M= zona de riesgo moderada	Asumir, Reducir	Control Interno cumplimiento de la ley
Suplantación/Reemplazo no autorizado	4	4	E= zona de Riesgo Extrema	Cumplimiento Art. 38	2	4	M= zona de riesgo moderada	Asumir, Reducir	Control Interno cumplimiento de la ley
Amenaza/soborno/influencia externa	4	4	E= zona de Riesgo Extrema	Cumplimiento Art. 38 – Art 453 Código Procedimiento penal	2	4	M= zona de riesgo moderada	Asumir, Reducir	Socialización y capacitación de la ley
Ausencia de Personal capacitado para la toma de entrevista	4	4	E= zona de Riesgo Extrema	Cumplimiento Art. 38	2	4	M= zona de riesgo moderada	Asumir, Reducir	Control Interno cumplimiento de la ley
No existencia de Unidad Militar para presentación de desmovilizados y toma de entrevista	1	4	M= zona de riesgo moderada	Ley 1621/2013 (ver anexo B)	1	4	M= zona de riesgo moderada	Asumir, Reducir	Control Interno cumplimiento de la ley

Fuente: autores

Para obtener un riesgo residual a partir del riesgo inherente existente, se deberán implementar los controles mencionados los cuales minimizarían el riesgo; Esta implementación de controles es tal como se definió en la página 45 de este documento los cuales disminuyen la probabilidad.

Con todo esto se observa que los controles disminuyen la probabilidad lo que minimiza el riesgo, generando un efecto transformador del proceso de entrevistas del personal desmovilizado.

Con estos controles aplicados a los tres activos de información que se viene analizando, se genera una nueva matriz de análisis de Riesgo (ver anexos K – L – M)

Cuadro 31. Nueva matriz análisis de riesgo promedio

		Probabilidad de Amenaza		
		Confidencialidad	Integridad	Disponibilidad
Magnitud de Daño	Datos e Información	8	4	4
	Sistemas e Infraestructura	6	4,5	3
	Personal	4	8	6

Fuente: autores

Habiendo disminuido el valor representativo del riesgo, cuadro 31, se realiza un análisis costo beneficios de la implementación de estos controles, teniendo en cuenta tres puntos relevantes, que garantizan el éxito de la institución y el cumplimiento de la misión constitucional, los cuales se logran gracias a la implementación de la metodología:

– Prestigio de la Institución: después de haber soportado un hecho como el mal llamado hacker “Andrés Sepúlveda”, donde el nombre de la Institución quedo por el suelo y como consecuencia del mismo el ejército nacional perdió credibilidad del pueblo Colombiano, y sufrió consecuencias políticas, se ve la necesidad de aprender de estos errores, de no ser reactivos sino proactivos y aplicar todos los recursos tanto materiales como personales en el tema propuesto, con el fin de evitar otra situación de estas y aunque la investigación arrojo responsables, la reputación del Ejercito quedo en una mala posición.

– Población persona protegida y derecho a la intimidad y buen nombre: gracias a la metodología se garantizara el deber constitucional y legal de proteger a la población desmovilizada, puesto que estos al acogerse al programa de

desmovilización se vuelven objetivo militar de los GAOML, además de garantizarle a estas personas el artículo 15 de la constitución nacional y su derecho a la intimidad personal y familiar y a su buen nombre, evitando así por fuga de información, poner en peligro la integridad de estas personas y las de sus familias creando un ambiente de seguridad en ellas, requisito indispensable para pasar a la legalidad.

- Propias tropas: se asegura la integridad de las personas o del servidor público que realiza el proceso de entrevista, puesto que, con los códigos implementados y asignados en el formato de entrevista, sumado al conocimiento de la norma por parte de este personal, se obtiene la conciencia del funcionario y el deber ser en todas las actuaciones, garantizando en el militar un ejemplo para la sociedad.

A lo anterior se suma que, si se establecen estos objetivos, se aumenta también el número de desmovilizaciones individuales por el simple hecho de ser más confiables, se aumenta el poder de combate producto de la información depositada en la entrevista y su buen manejo, se aumentan las operaciones militares y de desmovilización logrando reducir los GAOML y se previene el reclutamiento ilícito dándole la oportunidad a los jóvenes de tener opciones de educación, deporte y cultura.

4.3 FASE 3: RECOMENDACIONES ADMINISTRACIÓN DEL RIESGO

Para lograr ese efecto transformador en el proceso de entrevistas se recomienda

- Acatar la ley 1712 del 2014 en relación a la implementación de un programa de gestión documental (ver anexo D).

- Implementar un repositorio único de información de acuerdo a lo reglamentado en el artículo 28 de la Ley 1621 de 2013 (ver anexo B) y el artículo 15 del decreto 857 de 2014.

- Verificar la existencia de las actas de compromiso de reserva de todo el personal de acuerdo a lo reglamentado en la ley 1621 de 2013 articulo 38 (ver anexo B.

- Realizar lo necesario para garantizar el cumplimiento del decreto 857 de 2014 – articulo 20 con relación a estudios de credibilidad y confiabilidad.

- Acatar e implementar la política de seguridad del MDN – DIR2014-18 del 19 de junio de 2014 y realizar todo lo necesario para su socialización y cumplimiento.

– Para el envío de información digital con clasificación reservada es recomendable el uso de estampas de tiempo que permitan demostrar que serie de datos han existido y no han sido alterados desde un instante específico en el tiempo.

– Firmar digitalmente mediante una función hash que incluya una llave de encriptación los documentos digitales que se envíen mediante un enlace de comunicación no seguro

– Uso de tecnologías DLP que permitan permite prevenir la revelación intencional o involuntaria de información sensitiva “en reposo”, “en uso” o “en movimiento” hacia partes no autorizadas.

– Uso de soluciones VPN en los hogares de paz u otros sitios remotos que permita comunicarse de manera privada y segura en un medio no seguro como es internet.

– Validación del uso de la red de alta velocidad del gobierno colombiano – RAVEC para el envío de información, desde los hogares de paz.

5. METODOLOGÍA PARA LA CUSTODIA DE LAS ENTREVISTAS MILITARES DEL PERSONAL DESMOVILIZADO

La metodología para la custodia de las entrevistas militares del personal desmovilizado, es una serie de actividades que tiene por finalidad poder dar solución a los inconvenientes de seguridad presentados frente a la realización de las entrevistas del personal desmovilizado.

Esta metodología cubre las actividades a desarrollar teniendo en cuenta los aspectos normativos, tecnológicos, de talento humano y entorno, focos a partir de los cuales se diseñarán medidas y procedimientos claros que junto con la política general será de estricto cumplimiento.

Para la elaboración de esta metodología se tendrán en cuenta estas consideraciones:

- La metodología para la custodia de las entrevistas militares del personal desmovilizado es un documento de trabajo y como tal será accesible a todo el personal que requiera su utilización por lo que la información que se incluye no será limitada o clasificada

- Esta metodología se ajustará en todo momento al sistema de seguridad diseñado e implementado por el MDN – DIR2014-18 del 19 de junio de 2014.

- Su redacción es simple para que sea de comprensión de todos los involucrados en su cumplimiento.

- Tiene un carácter impositivo por lo cual se evitaron términos que no impliquen obligatoriedad

- Se deberá mantener actualizada.

MINISTERIO DE DEFENSA NACIONAL
GRUPO DE ATENCIÓN HUMANITARIA AL DESMOVILIZADO

Metodología para la custodia de las entrevistas militares del personal desmovilizado, desde las unidades tácticas de las fuerzas militares hasta el grupo de atención humanitaria al desmovilizado

	Elaborado	Elaborado	Aprobado
Nombre	John Alexander Lamprea Hernández	John Neider Orozco Gómez	Mauricio Ricardo Zúñiga Campo
Cargo	Ingeniero de Sistemas – Especialista Seguridad Informática	Teniente - Ingeniero de Sistemas – Especialista Seguridad Informática	Brigadier General - Coordinador Grupo de Atención Humanitaria al Desmovilizado
Firma			
Fecha	Junio 2015	Junio 2015	Junio 2015

5.1 ALCANCE

La presente metodología es aplicable en su totalidad a las unidades tácticas de las fuerzas militares y al Grupo de Atención Humanitaria al Desmovilizado.

Las políticas expresadas en este documento son de obligatorio cumplimiento para todo el personal que esté vinculado con el proceso entrevistas militares del personal desmovilizado.

5.2 CARACTERIZACIÓN DEL SISTEMA INFORMÁTICO

El sistema informatico para las entrevistas militares del personal desmovilizado SIGAHD, esta conformado por 6 módulos: entrevista militar, identificación, juridica, atención primaria, hogares y el módulo de administración. Esta es una aplicación web que funciona en la red del MDN, el cual cuenta con un servidor que reposa en las instalaciones del CAN- Bogotá en el cual se encuentra el aplicativo y la base de datos.

El acceso al Sistema de Información se genera por medio del módulo de administración, previa coordinación y visto bueno del coordinador del GAHD, este módulo arroja un pin y una contraseña y por defecto el administrador del sistema le delega un usuario que será en mayúsculas la primera letra del nombre y seguido del primer apellido completo. Es de anotar que esta información le llegará automaticamente al correo institucional del servidor público.

Asi las cosas los usuarios alimentan el sistema de información en tiempo real y en linea desde sus estaciones de trabajo ubicadas en el centro internacional Bogotá, y dichas estaciones conectadas por medio de una fibra óptica al centro de cómputo del MDN en el CAN. Se aclara que la información que se recoje en los hogares de paz, y unidades militares, viaja digitalizada por medio de un correo electronico y después en forma de expediente fisico, con el fin de agilizar procesos.

En la oficina del GAHD se cuenta con estaciones de trabajo distribuidas en el centro internacional conectadas a la red del MDN.

En las unidades tacticas se cuenta con estaciones de trabajo conectadas a la red del ejercito nacional.

Los servicios de red habilitados en las oficinas tanto del GAHD y de las unidades tacticas son muy limitadas, llegado el caso solo correo institucional, e intranet, de acuerdo a las necesidades de los usuarios y a la función que realizan.

La conexión con el exterior se realiza disponiendo de internet y por medio de mensajeria de la empresa 472.

El intercambio de informacion tanto interna como externa se realiza basicamente a traves de los correos institucionales, teniendo en cuenta que en los ultimos años el MDN viene implementando el sistema de información electronico de archivo SGDEA, que es el mecanismo por el cual internamente se esta manejando las comunicaciones oficiales e inclusive las peticiones, quejas y reclamos PQRS; pero tambien se intercambia información por medio de inspecciones judiciales de los entes pertinentes del estado.

La informacion ordinaria se procesa en las estaciones de trabajo de los usuarios y la informacion clasificada en las secciones o dependencias autorizadas como lo son el área de expedientes, juridica, archivo y de entrevistas ubicadas en las oficinas del centro internacional en Bogotá.

La informacion recibida desde las dependencias y las que se envia a los organismos de control del estado, que requieran la información o en su defecto a las fuerzas militares, se tramita por medio del sistema de información SIGAHD y en muchas ocasiones se tramita manualmente por medio de la oficina de archivo (En el caso de que sea necesario la verificacion de los expedientes fisicos de desmovilizados)

El personal que opera los equipos de computo posee los conocimientos y la preparacion necesaria para sus funciones con un nivel basico de escolaridad, basicamnete los procesos se aprenden de manera repetitiva.

5.3 RESULTADO DEL ANALISIS DE RIESGOS

Los bienes informaticos analisados son:

- El formato de entrevista.

- Los equipos de computo con el que se realizan las entrevisats en los hogares de paz y en las undiades militares.

- El personal/ funcionario publico/ entrevistador.

Las amenazas mas importantes a considerar de acuerdo al impacto son:

Formato:

- Fuga de informacion.
- Accesos no autorizados al formato digital.
- Alteracion/modificacion de las preguntas.
- Destruccion/plagio.

Equipo de computo:

- Accesos a dispositivos externos.
- Uso de equipos de terceros o externos.
- Uso de software no licenciado.
- No uso de software antivirus/antispyware.
- Rutinas de mantenimiento preventivo y correctivo.
- Traslado de equipos de computo de la institucion sin autorizacion.

Personal/funcionario/Entrevistador:

- Suplantacion/reemplazos no autorizados.
- Amenazas, sobornos, Influencia Externa.
- Cumplimiento de los articulos 36-37-38 de la ley 1621 del 2013 (ver anexo B).
- Ausencia de personal capacitdo o unidad militar para la toma de la entrevista.

Todo esto afectando la integridad, confidencialidad y disponibilidad de la informacion.

5.4 POLITICA GENERAL

- El proceso de entrevista se realizará con un estricto cumplimiento de la reserva legal y clasificación de la información, manejo de la información confidencial/sensible y de la información con carácter de datos personales.

- Todos los equipos informaticos sera indentificados y controlados fisicamente hasta nivel de componentes y/o perifericos.

- El aceso a las tecnologias (equipos o sistemas) sera expresamente aprobado y los usuarios responderan por su proteccion y buen uso teniendo la obligacion de informar cualqueir incidente o violacion que se produzca.

5.5 MEDIDAS Y PROCEDIMIENTOS

5.5.1 Medidas

- La ley 1621 del 2013 (ver anexo B) – ley de inteligencia y contra inteligencia será publicada y dada a conocer a todo el personal involucrado

- La clasificación y rotulado de la información y documentos se debe hacer de forma clara y visible teniendo en cuenta lo consignado en el artículo 11 del Decreto 857 del 2 de mayo del 2014 (ver anexo C).

- El respeto y protección del personal desmovilizado se garantizará de acuerdo al artículo 15 de la constitución política de Colombia y a la ley 1581 del 2012 – ley de protección de datos personales (ver anexo A).

- Los documentos emitidos por el MDN y la oficina asesora de sistemas OSA para el GAHD con relación a la seguridad de la información, se deberán dar a conocer y se deberán aplicar sin excepciones.

- Las area funcionales de GAHD se definirán por medio de documento dirigido al Grupo de Desarrollo Organizacional (GDO).

- Incluir en el plan anual de inversion del GAHD los equipos tecnológicos necesarios para garantizar la continuidad de las operaciones.

- La aplicabilidad de técnicas de poligrafo permitira al proceso militar la toma de decisiones en cuanto a la permanencia y la especialización del funcionario que realiza la entrevista.

- El plan de capacitación al enemigo se desarrollara periodicamente consigando en actas los compromisos y resultados del mismo.

- El aceso a las area de demovilización y los equipos de computo usados para las entrevistas deberan ser de acceso restrigido.

- El jefe del área de desmovilización como dueño del proceso analizará y medirá los respectivos controles definidos para garantizar su eficiencia y o re-definición.

5.5.2 Procedimientos

- Procedimiento No 1. Publicacion Leyes, normas y comunicados.

- La oficina asesora de sistemas, en coordinación con el coordinador del GAHD, desarollarán campañas visuales, eductivas, pedagogicas; con el fin de concientizar a los funcionarios acerca de la política de seguridad y la responsabilidad de cada servidor publico, ademas de evaluar su desempeño y compromiso con la seguridad informatica.

- Las circulares emitidas por la coordinación, deberán tener soportes juridicos claros y legales de acuerdo a la normatividad del GAHD y OAS.

- Los procedimientos del GAHD, deberán ser acordes a las leyes, normas y comunicados emitidos, y no se dejará ningun proceso sin su control y monitoreo.

- Responsable: Coordinador, OAS, sección juridica, talento humano.

- Procedimiento No 2. Rotulado y Clasificacion de la información

Se entiende por su función y naturaleza y por la ley de inteligencia y contrainteligencia, que toda información que llegue a las dependencias del GAHD, sera clasificada como reservada.

Responsable: Coordinador, Jefe del área de Desmovilización.

- Procedimiento No 3. Manejo de Documentos y Expedientes

- En el formato de entrevista del GAHD, para el personal Desmovilizado, se debe plasmar de forma clara y legible el código del entrevistador y/o en su defecto la persona que realiza la entrevista en modo, tiempo y lugar con el fin de que la persona que manipule la entrevista conozca el tratamiento que debe dársele y sus implicaciones.

- Una vez llegado el expediente administrativo al GAHD, el personal idóneo debe verificar la originalidad del documento (entrevista), por medio de una confrontación de identificación con registraduría y darle tramité de acuerdo al proceso del GAHD, mediante documento con fecha y responsable del mismo, así mismo deberá quedar registrada la respectiva trazabilidad en el sistema de información del grupo de atención humanitaria al desmovilizado (SIGAHD) y llenado todos los campos

del módulo de identificación, entrevista (segunda entrevista), jurídica (CODA) y archivo, consiguiendo con esto la trazabilidad del documento.

- Cuando el CODA (comité operativo para la dejación de armas), emita el concepto de Desmovilización, la secretaria técnica de este organismo entregará el expediente con la entrevista a la sección de archivo, quedando registrado la hora, fecha y responsable de este acto, así como también deberá quedar registrada trazabilidad en el SIGAHD, con su respectivo responsable y en tiempo real.

- La sección de archivo complementará todo el expediente de acuerdo a la ruta de desmovilización, lo organizará de acuerdo a lo dispuesto por la ley de archivo y lo digitalizará, lo cargará al repositorio en donde reposará, así como también el expediente físico original, deberá ser remitido a la empresa Thomas (MTI), de acuerdo al contrato de custodia de archivo, se le exigirá a este tercero el monitoreo de los expedientes por medio de cámaras de video y se nombrara en el GAHD un servicio “control cámaras” con la orden del día.

- La sección de archivo será la encargada de las inspecciones judiciales, previa aprobación del Sr. Coordinador y a la sección jurídica del GAHD, desarrollará los protocolos de entrega de información del GAHD en cumplimiento a la disposición que regula la entrega de información a las entidades del estado.

- Se exigirá por medio de un radiograma a las unidades tácticas que el expediente de la persona desmovilizada debe allegarse al GAHD en presencia de un funcionario de inteligencia que la unidad delegue evitando así fuga de información. Como medida de coordinación la unidad deberá informar previamente al GAHD que funcionario o agente de inteligencia es el encargado de este proceso y el GAHD deberá dejar constancia en modo, tiempo y lugar de la entrega de esta información.

Responsable: Coordinador, jefe del Área de Desmovilización, Jefe del Área de Atención Primaria.

- Procedimiento No 4. Manejo de equipos tecnológicos e información

- La oficina asesora de sistemas OAS instalará en cada uno de los equipos de cómputo agentes para el monitoreo de las impresiones realizadas por los usuarios y se configure el software antivirus con la política necesaria para restringir unidades de CD/DVD y USB.

- El coordinador de GAHD mediante circular de seguridad firmada especificará los usuarios autorizados para utilizar recursos tecnológicos del ministerio y donde se prohíben el uso de equipos de cómputo personales y medios de almacenamiento externo.

- El coordinador del GAHD mediante circular y en concordancia con la parte jurídica denotará las restricciones y las implicaciones a las cuales se deben ajustar los funcionarios.

- Para garantizar la continuidad del negocio se suministrará nuevas tecnologías, así como sistemas de almacenamiento y backups.

- Frente a seguridad de redes, configurar todo lo relacionado con seguridad perimetral, firewall y sistemas antivirus y anti spyware.

- Unificar con los hogares de paz un medio seguro de transmisión de la entrevista militar, desde estos al GAHD, así como también fijar canales de transmisión con el fin de garantizar emisión y recepción adecuada de la entrevista militar y/o designar responsables por medio de un acto administrativo legal, para que sea entregada personalmente en sobre sellado, junto con el expediente administrativo al GAHD, o en lo posible garantizar la conexión por medio de VPN para utilizar los recursos del MDN y poder monitorear el flujo de paquetes de información.

- Crear las reglas necesarias de seguridad para la protección de la entrevista en el file server y mediante una tecnología, prevenir la perdida de datos y poder monitorear los mismos en coordinación con la oficina asesora de sistemas.

- El administrador del sistema debe enviar al jefe de seguridad del GAHD los log de auditoría y posibles alarmas de infracción del protocolo, este a su vez realizará un análisis de esta información y tomará las medidas pertinentes de acuerdo a la circular de seguridad de la información y la ley.

- El módulo de entrevistas se desarrollará mediante órdenes de trabajo al desarrollador de software con el fin de que se diseñe e implemente de forma digital con un hash que garantizará la originalidad del documento.

- El responsable de la sección de sistemas previa reunión con los jefes de área en especial con el proceso de la entrevista definirá los usuarios con sus respectivos roles dentro del SIGAHD, esto será aprobado y socializado por la orden del día de GAHD, el cual es un documento jurídico.

- Se desarrollará un plan de capacitación a todo el personal del estricto cumplimiento a los criterios y comportamientos que deben seguir todos los funcionarios y cualquier persona que tenga una relación contractual con el sector defensa o que tenga acceso a los activos de información, con el propósito de preservar la confidencialidad, integridad y disponibilidad de la información

– La OAS realizará campañas de las mejores prácticas de seguridad de la información donde de forma pedagógica, sencilla y clara informará a los funcionarios acerca de la política y sus implicaciones.

Responsable: administrador de sistemas y Jefe de seguridad del GAHD

– Procedimiento No 5. Manejo de Recursos Humanos

– Antes de la contratación se investigará los antecedentes penales y de comportamiento del personal civil.

– Se llevarán semestralmente pruebas de polígrafo a todo el personal que tenga que ver con el procedimiento de entrevista militar.

– Se garantizará la continuidad de los funcionarios en el proceso de la entrevista y mantendrá actualizada la carpeta de actas compromiso de confidencialidad de todo el personal.

– Las funciones del oficial de servicio deberán estar enmarcadas dentro del ámbito de la ley en la parte de seguridad.

– La identificación del personal de la dependencia se hará con un elemento de identificación, fichero autorizado por el coordinador del GAHD con el fin de identificar personal autorizado.

– El uso de los planes de educación no formal existentes en el MDN será obligatorio para los funcionarios que intervienen en el proceso de entrevista al desmovilizado.

Responsable: jefe del área de desmovilización

6. PROPUESTA TÉCNICA PARA LA ADQUISICIÓN DE SOLUCIÓN ESPECIALIZADO QUE PERMITA EJERCER CONTROLES SOBRE LOS RIESGOS IDENTIFICADOS

6.1 BENCHMARKING

De acuerdo a lo tratado durante todo el documento y a lo expuesto en las sugerencias es también necesaria la implementación de una infraestructura tecnológica que permita el cumplimiento de las políticas de seguridad y tratamiento de documentos del ministerio de defensa nacional MDN.

El alcance del proyecto supone una propuesta tecnológica especializada que permita evitar la fuga de información de las entrevistas militares del personal desmovilizado del grupo de atención humanitaria.

La propuesta tecnológica se basa en un sistema DLP para garantizar la confidencialidad de la información pudiendo detectar riesgos de fuga de información de datos confidenciales, proteger los datos sin importar su almacenamiento o definición en la escala para la definición de datos y un sistema de comunicación VPN que permita garantizar la privacidad cuando se esté trasmitiendo por una red que no sea de confianza.

Con el fin de garantizar la mejor herramienta tecnológica en el mercado en la actualidad se realizó el análisis de los requisitos funcionales del GAHD con base en el cuadrante mágico de Gartner para el manejo de firewall y para el manejo de sistemas DLP. Ver figura 3 y 4.

Figura 3. Cuadrante mágico de gartner enterprise-network-firewalls

Fuente: Gartner[38]

Estas fortalezas y precauciones presentadas en el informe “Enterprise-Network-Firewalls se reúnen en las ilustraciones 32 y 33.

[38] GARTNER. Magic Quadrant for Enterprise Network Firewalls. [En línea]. [Consultado el 6 de febrero de 2016]. Disponible en; http://innetworktech.com/wp-content/uploads/2015/04/Magic-Quadrant-for-Enterprise-Network-Firewalls.pdf

Cuadro 32. Fortalezas y precauciones presentadas en el informe “cuadrante de enterprise-network-firewalls

Proveedor	Fortalezas	Precauciones
CheckPoint software Technologies	Firewall CheckPoint obtienen constantemente altas puntuaciones de los clientes en materia de seguridad y facilidad de gestión en entornos complejos.	El precio es el factor más común invocado por los clientes de Gartner para introducir la competencia para CheckPoint
	Se sigue invirtiendo en su suite de gestión, con varias funciones de la versión R80 destinada a mejorar la capacidad de auditoría y capacidad de gestión de la política de seguridad, y que finalmente se ha combinado los componentes de la red y de las aplicaciones en una política unificada	Los clientes de CheckPoint a menudo son lentas en adoptar nuevas opciones de software
Palo Alto Networks	Facilidad de uso y calidad	Informe de rendimiento del antivirus no es creíble
	Los cortafuegos y el IPS están estrechamente integrados,	La empresa debe desarrollar un mejor ecosistema de soporte de productos de terceros

Fuente: autores

Figura 4. Cuadrante mágico de gartner DLP's

Fuente: Gartner[39]

Fortalezas y precauciones presentadas en el informe “Enterprise Data Loss Prevention”

[39] GARTNER. Magic Quadrant for Enterprise Data Loss Prevention. [En línea]. [Consulta 6 de febrero de 2016]. Disponible en: https://www.gartner.com/doc/reprints?id=1-2X9K7Y 9&ct= 160128&st=sb

Cuadro 33. Fortalezas y precauciones presentadas en el informe “cuadrante de enterprise data loss prevention

Proveedor	Fortalezas	Precauciones
Symantec	Symantec ofrece las técnicas más completas de detección de datos sensibles en el mercado, con una funcionalidad avanzada que puede cubrir una gran amplitud de escenarios de pérdida de datos	monitoreo y descubrimiento de datos sensibles en aplicaciones en la nube de Symantec es basada en puntos finales,
	Symantec es compatible con un modelo de implementación híbrida para varios de sus productos DLP,	
Forcepoint	Forcepoint apoya el descubrimiento de contenido confidencial almacenada en la caja, Microsoft Exchange Online y Microsoft SharePoint Online mediante las API nativas.	La participación de Raytheon en el mercado de defensa puede ayudar a revitalizar Forcepoint con inteligencia y productos adicionales (por ejemplo, SureView privilegiada de amenazas); Sin embargo, todavía está llena de riesgo de ejecución

Fuente: autores

7. CONCLUSIONES

Es de vital importancia para una organización, que los funcionarios conozcan las políticas que rigen la misma y las implicaciones que conllevan el desacato de una directriz. Se ve que en el GAHD no existen políticas claras definidas, ni procedimientos y políticas establecidos que prevengan la fuga de información.

Los funcionarios del GAHD en especial el área de Desmovilización desconocen la normatividad que los rige en materia de funciones, objetivos y procesos de Inteligencia.

Si bien el Ministerio de Defensa Nacional cuenta con una oficina especializada en el área de Sistemas llamada Oficina Asesora de Sistemas- OAS, con un full de ingenieros especializados en las ramas de la ingeniería, no cubre la totalidad de las dependencias del Ministerio de Defensa Nacional, dejando a la oficina del Grupo de Atención Humanitaria, oficina descentralizada pero que cuenta con recursos informáticos asignados por el MDN, sin respaldo técnico en materia de seguridad de información. Se debe siempre verificar que la seguridad no se da a medias sino es un proceso completo.

Es importante la socialización, difusión, capacitación, apoyo y recomendación en materia de seguridad de la información y mejores prácticas a todo nivel por parte de la OAS, utilizando las diferentes estrategias como pantallas, correo electrónico, campañas interactivas y simulacros, en colaboración con el personal de talento humano.

La OAS, debe dar a conocer y ofrecer los servicios con los que cuenta en SW, HW, personal, asesorías, a todo nivel, con el fin de que se utilicen estos recursos en todas las dependencias para prevenir fugas de información.

Se debe reevaluar el personal que interactúa con el proceso de DDR en especial con la entrevista del personal desmovilizado, puesto que se requiere personal idóneo, con conocimientos, compromiso y fe en la causa para el desarrollo de esta labor, además de la reserva del caso y la integridad como servidores públicos.

El ministerio de defensa debe reforzar con personal idóneo, las dependencias que requieren por su concepción y misión, mayor uso de las tecnologías para prevenir la fuga de información y aseguramiento de sus bienes informáticos.

Si bien existe una matriz cadena de valor Vs responsabilidad del GAHD, en donde se menciona el ciclo PHVA y se evidencia la fuga de información como un elemento del verificar, no se cuenta controles para mitigar este riesgo además de no haberle dado tratamiento a este.

La seguridad somos todos, se deben unir esfuerzos para atacar en los diferentes flancos los riesgos, a los cuales puede estar expuesta la institución en un momento dado; además de implementar controles y medidas disuasivas y prever el futuro.

8. EFECTO TRANSFORMADOR DEL PROYECTO

Todo lo contenido en este documento el cual es producto de los trabajos de campo con el personal del grupo de atención humanitaria al desmovilizado, análisis e identificación de falencias y generación de recomendaciones para mejorar los procesos a partir de controles ha permitido a la dirección del GAHD tomar decisiones acertadas y garantizar el cumplimiento misional y con este aportar a la labor constitucional de la fuerza.

Estas decisiones han sido desde el mejoramiento del proceso de las entrevistas garantizando los tres pilares de la seguridad de la información: disponibilidad, integridad y confidencialidad hasta la identificación de la necesidad de implementaciones, desarrollos de software y adquisición de hardware, pasando por el fortalecimiento de los sistemas de información con el conocimiento socialización y capacitación del personal en la directiva ministerial 18-2014 “política de seguridad”.

Se ha logrado una sinergia entre las dependencias del MDN, especialmente la Oficina asesora de sistemas con el GAHD, mejorando el clima organizacional y llevando la institución hacia los niveles de seguridad óptimos para su funcionamiento.

Por último, se logra conciencia, disciplina, cultura y compromiso en el personal que labora en el GAHD, pues con el conocimiento de la normatividad que rige la seguridad de la información en el MDN y que respalda la labor de Inteligencia, más las implicaciones de su desobedecimiento, se obtienen productos más eficientes y eficaces satisfaciendo la necesidad de los clientes.

Todo esto certificado mediante comunicado que remite el Brigadier General Mauricio Ricardo Zúñiga Campo, coordinador del grupo de atención humanitaria al desmovilizado a la Universidad Piloto de Colombia – Anexo N.

BIBLIOGRAFÍA

BORTNIK Sebastián. ¿Qué es la fuga de Información? – ESET. [En línea]. [consultado el 16 de enero del 2016]. Disponible en: http://www.welivesecurity.com/la-es/2010/04/13/que-es-la-fuga-de-informacion/

CALVO MOYANO, Arantxa. Fuga de información, la mayor amenaza para la reputación corporativa. [En línea]. [Consultado el 24 enero de 2016]. Disponible en: http://www.redseguridad.com/opinion/articulos/fuga-de-informacion-la-mayor-amenaza-para-la-reputacion-corporativa

CERT. Hashing. [En línea]. [Consultado el 29 de enero de 2016]. Disponible en www.cert.fnmt.es/content/pages_std/html/tutoriales/tuto7.htm

COLOMBIA. Alcaldía de Bogotá. Ley 1581 del 17 de octubre de 2015: Protección de datos personales. [En línea]. [Consultado el 16 de enero del 2016]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

_____. Plan Nacional de Desarrollo. [en línea]. [Consultado el 24 de enero de 2016]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=8795

COLOMBIA. Presidencia de la República. Decreto 857 de 2104. [En línea]. [Consulta el 16 de enero de 2016]. Disponible en: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%2 01712 %20DEL%2006%20DE%20MARZO%20DE%202014.pdf

_____. Ley 1621 del 17 de abril de 2013: Ley de Inteligencia y Contra Inteligencia. [En línea]. [Consultado el 16 de enero 2016]. Disponible en: http://wsp.presidencia.gov.co/Normativa/ Leyes/Documents/2013/LEY%201621%20DEL%2017%20DE%20ABRIL%20DE% 202013.pdf

_____. Ley de transparencia - Ley 1712 del 06 de marzo de 2014. [En línea]. [consultado el 16 de enero de 2016]. Disponible en http://wsp.presidencia.gov.co/ Normativa/Leyes/Documents/LEY%1712%20DEL%2006%20DE%20MARZO%20 DE%202014.pdf

COLOMBIA. Fuerzas Militares de Colombia Ejército Nacional. Manual de Calidad, versión 8, 2015. [En línea]. [consultado el 24 de enero de 2016]. Disponible en https://www. ejercito.mil.co/?idcategoria=227258#

COLOMBIA. Procuraduría General de la Nación. Constitución política de Colombia. [En línea]. [Consultado el 24 de enero de 2016]. Disponible en: http://www.procuraduria. gov.co/guiamp/ media/file/Macroproceso%20Disciplinario/ Constitucion_Politica_de_Colombia.htm

EL TIEMPO. Justicia; Operación Andrómeda. [En línea]. [Consultado el 16 de enero 2016]. Disponible en: http://www.eltiempo.com/politica/justicia/informe-militar-sobre-el-caso-andromeda/ 15141236.

EN COLOMBIA. Código Penal Militar. [En línea]. [Consultado el 24 de enero de 2016]. Disponible en: https://encolombia.com/derecho/codigos/penal-militar/

ESET. (2015). Tendencias 2015: El mundo corporativo en la mira. [En línea]. [Consultado el 24 de enero de 2016]. Disponible en: http://www.welivesecurity.com/wp-content/uploads/2015/01/ tendencias_ 2015_eset_mundo_corporativo.pdf

GARTNER. Magic Quadrant for Enterprise Network Firewalls. [En línea]. [Consultado el 6 de febrero de 2016]. Disponible en; http://innetworktech.com/wp-content/uploads/2015/04/Magic-Quadrant-for-Enterprise-Network-Firewalls.pdf

GUTIÉRREZ Amaya, Camilo. 10 años de fuga de información: conoce los incidentes para no repetir la historia. – ESET. [En línea]. [consultado el 16 de enero del 2016]. Disponible en http://www.welivesecurity.com/la-es/2015/01/08/10-anos-fuga-de-informacion/

IBM. Opciones de seguridad en la transmisión. [En línea]. [Consultado el 24 de enero de 2016]. Disponible en: http://www-01.ibm.com/support/knowledgecenter/ssw_ibm_i_71/ rzaj4/rzaj45zh crypto intro.htm?lang=es

INCODER Administración de Riesgos Corporativos. Técnicas de Aplicación Colombia. USA; Price Waterhouse Coopers, 2005. p. 39

INSTITUTO COLOMBIANO DE NORMAS ICONTEC. Norma Técnica Colombiana NTC-ISO31000. [En línea]. [Consultado el 24 de enero de 2016]. Disponible en: http://tienda.icontec.org/brief/NTC-ISO31000.pdf.

_____. Norma técnica colombiana ISO/IEC 27002. Tecnologías de Información – Técnicas de Seguridad – Guía de Prácticas de Controles de Seguridad de la Información. 2013. [En línea]. [consultado el 24 de enero de 2016]. Disponible en: www.**iso**27000.es/**iso**27000.html

IZENPE. Sellado de Tiempo. [En línea]. [Consultado el 29 de enero de 2016]. Disponible en www.izenpe.com/s15.../es/...sellado_tiempo/es.../servicios_de_ sellado _tiempo.html

JOHANSEN, B. Leaders Make the Future: Ten New Leadership Skills for an Uncertain World. San Francisco, USA: Berrett-Koehler Publisher, 2009 150 p.

MINISTERIO DEL TRABAJO Y SEGURIDAD SOCIAL. Guía para la administración del riesgo – DAFP [En línea]. [Consultado el 29 de enero de 2016]. Disponible en: http://portal.dafp.gov.co/portal/pls/portal/formularios.retrive_ publicaciones?no=1592

REAL ACADEMIA ESPAÑOLA. Diccionario de la lengua española | Edición del Tricentenario. Seguro. RAE. [En línea]. [Consultado el 16 de enero del 2016]. Disponible en http://dle.rae.es/?id=XTrgHXd

SOLÍS, Sergio. Prevención de fuga de datos: Un enfoque para el negocio. [En línea]. [Consultado el 24 de enero de 2016]. Disponible en: http://www.isaca.org/ chapters7/ Monterrey/ Events/Documents/20121025%20Preveci%C3%B3n%20 de%20Fuga% 20de%20Datos.pdf

ANEXOS

Anexo A. Ley 1581 de 2012

LEY ESTATUTARIA No. 1581 17 OCT 2012

"POR EL CUAL SE DICTAN DISPOSICIONES GENERALES PARA LA PROTECCIÓN DE DATOS PERSONALES".

EL CONGRESO DE COLOMBIA

DECRETA:

TÍTULO I

OBJETO, ÁMBITO DE APLICACIÓN Y DEFINICIONES

ARTÍCULO 1. Objeto. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

ARTÍCULO 2. Ámbito de aplicación. Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

La presente ley aplicará al Tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.

El régimen de protección de datos personales que se establece en la presente Ley no será de aplicación:

a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.

   Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los Responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley.

b) A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo.

ANEXO A. (continuación)

a) **Principio de legalidad en materia de Tratamiento de datos:** El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen.

b) **Principio de finalidad:** El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.

c) **Principio de libertad:** El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

d) **Principio de veracidad o calidad:** La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

e) **Principio de transparencia:** En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

f) **Principio de acceso y circulación restringida:** El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente Ley.

Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley.

g) **Principio de seguridad:** La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

h) **Principio de confidencialidad:** Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.

ANEXO A. (continuación)

TÍTULO III

CATEGORIAS ESPECIALES DE DATOS

ARTÍCULO 5. Datos sensibles. Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

ARTICULO 6.Tratamiento de datos sensibles. Se prohíbe el Tratamiento de datos sensibles, excepto cuando:

a) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.

b) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y éste se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.

c) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular.

d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

e) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

ARTÍCULO 7. Derechos de los niños, niñas y adolescentes. En el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.
Queda proscrito el Tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública.
Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del Tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás. El Gobierno Nacional reglamentará la materia, dentro de los seis (6) meses siguientes a la promulgación de esta Ley.

4

TÍTULO IV

DERECHOS Y CONDICIONES DE LEGALIDAD PARA EL TRATAMIENTO DE DATOS

ARTÍCULO 8. Derechos de los Titulares. El Titular de los datos personales tendrá los siguientes derechos:

a) Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.

b) Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley.

c) Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales.

d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen.

e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución.

f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

ARTÍCULO 9. Autorización del Titular. Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.

ARTÍCULO 10. Casos en que no es necesaria la autorización. La autorización del Titular no será necesaria cuando se trate de:

a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.

b) Datos de naturaleza públi.

c) Casos de urgencia médica o sanitaria.

d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.

e) Datos relacionados con el Registro Civil de las Personas.

5

Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley.

ARTÍCULO 11. Suministro de la información. La información solicitada podrá ser suministrada por cualquier medio, incluyendo los electrónicos, según lo requiera el Titular. La información deberá ser de fácil lectura, sin barreras técnicas que impidan su acceso y deberá corresponder en un todo a aquella que repose en la base de datos.

El Gobierno Nacional establecerá la forma en la cual los Responsables del Tratamiento y Encargados del Tratamiento deberán suministrar la información del Titular, atendiendo a la naturaleza del dato personal, Esta reglamentación deberá darse a más tardar dentro del año siguiente a la promulgación de la presente ley.

ARTÍCULO 12. Deber de informar al Titular. El Responsable del Tratamiento, al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa lo siguiente:

a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo.

b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando éstas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes.

c) Los derechos que le asisten como Titular.

d) La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.

Parágrafo. El Responsable del Tratamiento deberá conservar prueba del cumplimiento de lo previsto en el presente artículo y, cuando el Titular lo solicite, entregarle copia de esta.

ARTÍCULO 13. Personas a quienes se les puede suministrar la información. La información que reúna las condiciones establecidas en la presente ley podrá suministrarse a las siguientes personas:

a) A los Titulares, sus causahabientes o sus representantes legales.

b) A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.

c) A los terceros autorizados por el Titular o por la ley.

TITULO V

PROCEDIMIENTOS

ARTICULO 14. Consultas. Los Titulares o sus causahabientes podrán consultar la información personal del Titular que repose en cualquier base de datos, sea esta del sector público o privado. El Responsable del Tratamiento o Encargado del Tratamiento deberán suministrar a éstos toda la información

→

6

contenida en el registro individual o que esté vinculada con la identificación del Titular.
La consulta se formulará por el medio habilitado por el Responsable del Tratamiento o Encargado del Tratamiento, siempre y cuando se pueda mantener prueba de ésta.

La consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

Parágrafo. Las disposiciones contenidas en leyes especiales o los reglamentos expedidos por el Gobierno Nacional podrán establecer términos inferiores, atendiendo a la naturaleza del dato personal.

ARTICULO 15. Reclamos. El Titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en esta ley, podrán presentar un reclamo ante el Responsable del Tratamiento o el Encargado del Tratamiento el cual será tramitado bajo las siguientes reglas:

1. El reclamo se formulará mediante solicitud dirigida al Responsable del Tratamiento o al Encargado del Tratamiento, con la identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

2. Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga "reclamo en trámite" y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

3. El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

ARTICULO 16. Requisito de procedibilidad. El Titular o causahabiente sólo podrá elevar queja ante la Superintendencia de Industria y Comercio una vez haya agotado el trámite de consulta o reclamo ante el Responsable del Tratamiento o Encargado del Tratamiento.

7

ANEXO A. (continuación)

TÍTULO VI

DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO Y ENCARGADOS DEL TRATAMIENTO

ARTÍCULO 17. Deberes de los Responsables del Tratamiento. Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular.

c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.

d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.

f) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a éste se mantenga actualizada.

g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.

h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley.

i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.

j) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley.

k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos.

l) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.

m) Informar a solicitud del Titular sobre el uso dado a sus datos.„

8

n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

ARTÍCULO 18. Deberes de los Encargados del Tratamiento. Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley.

d) Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.

e) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente ley.

f) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares.

g) Registrar en la base de datos las leyenda "reclamo en trámite" en la forma en que se regula en la presente ley.

h) Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.

i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.

j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.

k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Parágrafo. En el evento en que concurran las calidades de Responsable del Tratamiento y Encargado del Tratamiento en la misma persona, le será exigible el cumplimiento de los deberes previstos para cada uno.

9

ANEXO A. (continuación)

TÍTULO VII

DE LOS MECANISMOS DE VIGILANCIA Y SANCIÓN

CAPÍTULO 1

DE LA AUTORIDAD DE PROTECCION DE DATOS

ARTÍCULO 19. Autoridad de Protección de Datos. La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley.

Parágrafo 1. El Gobierno Nacional en el plazo de seis (6) meses contados a partir de la fecha de entrada en vigencia de la presente ley incorporará dentro de la estructura de la Superintendencia de Industria y Comercio un despacho de Superintendente Delegado para ejercer las funciones de Autoridad de Protección de Datos.

Parágrafo 2. La vigilancia del tratamiento de los datos personales regulados en la Ley 1266 de 2008 se sujetará a lo previsto en dicha norma.

ARTÍCULO 20. Recursos para el ejercicio de sus funciones. La Superintendencia de Industria y Comercio contará con los siguientes recursos para ejercer las funciones que le son atribuidas por la presente ley:

a) Los recursos que le sean destinados en el Presupuesto General de la Nación.

ARTÍCULO 21. Funciones. La Superintendencia de Industria y Comercio ejercerá las siguientes funciones:

a) Velar por el cumplimiento de la legislación en materia de protección de datos personales.

b) Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos.

c) Disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el Titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva.

d) Promover y divulgar los derechos de las personas en relación con el Tratamiento de datos personales e implementará campañas pedagógicas para capacitar e informar a los ciudadanos acerca del ejercicio y garantía del derecho fundamental a la protección de datos.,

10

e) Impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento y Encargados del Tratamiento a las disposiciones previstas en la presente ley.

f) Solicitar a los Responsables del Tratamiento y Encargados del Tratamiento la información que sea necesaria para el ejercicio efectivo de sus funciones.

g) Proferir las declaraciones de conformidad sobre las transferencias internacionales de datos.

h) Administrar el Registro Nacional Público de Bases de Datos y emitir las órdenes y los actos necesarios para su administración y funcionamiento.

i) Sugerir o recomendar los ajustes, correctivos o adecuaciones a la normatividad que resulten acordes con la evolución tecnológica, informática o comunicacional.

j) Requerir la colaboración de entidades internacionales o extranjeras cuando se afecten los derechos de los Titulares fuera del territorio colombiano con ocasión, entre otras, de la recolección internacional de datos personales.

k) Las demás que le sean asignadas por ley.

CAPÍTULO 2

PROCEDIMIENTO Y SANCIONES

ARTÍCULO 22. Trámite. La Superintendencia de Industria y Comercio, una vez establecido el incumplimiento de las disposiciones de la presente ley por parte del Responsable del Tratamiento o el Encargado del Tratamiento, adoptará las medidas o impondrá las sanciones correspondientes.

En lo no reglado por la presente ley y los procedimientos correspondientes se seguirán las normas pertinentes del Código Contencioso Administrativo.

ARTICULO 23. Sanciones. La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:

a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó.

b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar.

c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio.

11

d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles.

Parágrafo. Las sanciones indicadas en el presente artículo sólo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva.

ARTICULO 24. Criterios para graduar las sanciones. Las sanciones por infracciones a las que se refieren el artículo anterior, se graduarán atendiendo los siguientes criterios, en cuanto resulten aplicables:

a) La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley.

b) El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción.

c) La reincidencia en la comisión de la infracción.

d) La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio.

e) La renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio.

f) El reconocimiento o aceptación expresos que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.

CAPÍTULO 3

DEL REGISTRO NACIONAL DE BASES DE DATOS

ARTÍCULO 25. Definición. El Registro Nacional de Bases de Datos es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país.
El registro será administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos.
Para realizar el registro de bases de datos, los interesados deberán aportar a la Superintendencia de Industria y Comercio las políticas de tratamiento de la información, las cuales obligarán a los responsables y encargados del mismo, y cuyo incumplimiento acarreará las sanciones correspondientes. Las políticas de Tratamiento en ningún caso podrán ser inferiores a los deberes contenidos en la presente ley.

Parágrafo. El Gobierno Nacional reglamentará, dentro del año siguiente a la promulgación de la presente Ley, la información mínima que debe contener el Registro, y los términos y condiciones bajo los cuales se deben inscribir en éste los Responsables del Tratamiento. //

12

TÍTULO VIII

TRANSFERENCIA DE DATOS A TERCEROS PAÍSES

ARTÍCULO 26. Prohibición. Se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios.
Esta prohibición no regirá cuando se trate de:

a) Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia.

b) Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública.

c) Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.

d) Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.

e) Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular.

f) Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

Parágrafo 1. En los casos no contemplados como excepción en el presente artículo, corresponderá a la Superintendencia de Industria y Comercio, proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. Para el efecto, el Superintendente queda facultado para requerir información y adelantar las diligencias tendientes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.

Parágrafo 2. Las disposiciones contenidas en el presente artículo serán aplicables para todos los datos personales, incluyendo aquellos contemplados en la Ley 1266 de 2008.

TÍTULO IX

OTRAS DISPOSICIONES

ARTICULO 27. Normas Corporativas Vinculantes. El Gobierno Nacional expedirá la reglamentación correspondiente sobre Normas Corporativas Vinculantes para la certificación de buenas prácticas en protección de datos personales y su transferencia a terceros países.

13

ANEXO A. (continuación)

ARTICULO 28. Régimen de transición. Las personas que a la fecha de entrada en vigencia de la presente ley ejerzan alguna de las actividades acá reguladas tendrán un plazo de hasta seis (6) meses para adecuarse a las disposiciones contempladas en esta ley.

ARTICULO 29. Derogatorias. La presente ley deroga todas las disposiciones que le sean contrarias a excepción de aquellas contempladas en el artículo segundo.

ARTICULO 30. Vigencia. La presente Ley rige a partir de su promulgación.

EL PRESIDENTE DEL HONORABLE SENADO DE LA REPÚBLICA

ROY LEONARDO BARRERAS MONTEALEGRE

EL SECRETARIO GENERAL DEL HONORABLE SENADO DE LA REPUBLICA

GREGORIO ELJACH PACHECO

EL PRESIDENTE DE LA HONORABLE CAMARA DE REPRESENTANTES

AUGUSTO POSADA SANCHEZ

LA SECRETARIA GENERAL (E) DE LA HONORABLE CAMARA DE REPRESENTANTES

FLOR MARINA DAZA RAMIREZ

14

ANEXO A. (continuación)

LEY ESTATUTARIA No. 1581

"POR EL CUAL SE DICTAN DISPOSICIONES GENERALES PARA LA PROTECCIÓN DE DATOS PERSONALES"

REPÚBLICA DE COLOMBIA - GOBIERNO NACIONAL

PUBLÍQUESE Y CÚMPLASE

En cumplimiento de lo dispuesto en la Sentencia C-748 de 2011 proferida por la Corte Constitucional, se procede a la sanción del proyecto de Ley, la cual ordena la remisión del expediente al Congreso de la República, para continuar el trámite de rigor y posterior envío al Presidente de la República.

Dada en Bogotá, D.C., a los 17 OCT 2012

LA MINISTRA DE JUSTICIA Y DEL DERECHO,

RUTH STELLA CORREA PALACIO

EL MINISTRO DE HACIENDA Y CRÉDITO PÚBLICO,

MAURICIO CÁRDENAS SANTA MARÍA

EL MINISTRO DE COMERCIO, INDUSTRIA Y TURISMO,

SERGIO DIAZ-GRANADOS GUIDA

EL MINISTRO DE TECNOLOGÍAS, DE LA INFORMACIÓN Y LAS COMUNICACIONES,

DIEGO MOLANO VEGA

LEY ESTATUTARIA No. 1621 17 ABR 2013

"POR MEDIO DEL CUAL SE EXPIDEN NORMAS PARA FORTALECER EL MARCO JURÍDICO QUE PERMITE A LOS ORGANISMOS QUE LLEVAN A CABO ACTIVIDADES DE INTELIGENCIA Y CONTRAINTELIGENCIA CUMPLIR CON SU MISIÓN CONSTITUCIONAL Y LEGAL, Y SE DICTAN OTRAS DISPOSICIONES".

EL CONGRESO DE LA REPUBLICA

DECRETA:

CAPÍTULO I
PRINCIPIOS GENERALES

ARTÍCULO 1. OBJETO Y ALCANCE. La presente Ley tiene por objeto fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir adecuadamente con su misión constitucional y legal. Establece los límites y fines de las actividades de inteligencia y contrainteligencia, los principios que las rigen, los mecanismos de control y supervisión, la regulación de las bases de datos, la protección de los agentes, la coordinación y cooperación entre los organismos, y los deberes de colaboración de las entidades públicas y privadas, entre otras disposiciones.

ARTÍCULO 2. DEFINICIÓN DE LA FUNCIÓN DE INTELIGENCIA Y CONTRAINTELIGENCIA. La función de inteligencia y contrainteligencia es aquella que desarrollan los organismos especializados del Estado del orden nacional, utilizando medios humanos o técnicos para la recolección, procesamiento, análisis y difusión de información, con el objetivo de proteger los derechos humanos, prevenir y combatir amenazas internas o externas contra la vigencia del régimen democrático, el régimen constitucional y legal, la seguridad y la defensa nacional, y cumplir los demás fines enunciados en esta Ley.

ARTÍCULO 3. ORGANISMOS QUE LLEVAN A CABO LA FUNCIÓN DE INTELIGENCIA Y CONTRAINTELIGENCIA. La función de inteligencia y contrainteligencia es llevada a cabo por las dependencias de las Fuerzas Militares y la Policía Nacional organizadas por éstas para tal fin, la Unidad de Información y Análisis Financiero (UIAF), y por los demás organismos que faculte para ello la Ley. Estos organismos conforman la comunidad de inteligencia y son los únicos autorizados para desarrollar actividades de inteligencia y contrainteligencia. Todos los organismos que lleven a cabo estas actividades estarán sujetos al cumplimiento de la presente ley de manera integral.

ARTÍCULO 4. LÍMITES Y FINES DE LA FUNCIÓN DE INTELIGENCIA Y CONTRAINTELIGENCIA. La función de inteligencia y contrainteligencia estará limitada en su ejercicio al respeto de los derechos humanos y al cumplimiento estricto de la Constitución, la Ley y el Derecho Internacional Humanitario y el Derecho Internacional de los Derechos Humanos. En especial, la función de inteligencia estará limitada por el principio de reserva legal que garantiza la protección de los derechos a la honra, al buen nombre, a la intimidad personal y familiar, y al debido proceso.

Ninguna información de inteligencia y contrainteligencia podrá ser obtenida con fines diferentes de:

Anexo B. (continuación)

a. Asegurar la consecución de los fines esenciales del Estado, la vigencia del régimen democrático, la integridad territorial, la soberanía, la seguridad y la defensa de la Nación;
b. Proteger las instituciones democráticas de la República, así como los derechos de las personas residentes en Colombia y de los ciudadanos colombianos en todo tiempo y lugar –en particular los derechos a la vida y la integridad personal– frente a amenazas tales como el terrorismo, el crimen organizado, el narcotráfico, el secuestro, el tráfico de armas, municiones, explosivos y otros materiales relacionados, el lavado de activos, y otras amenazas similares; y
c. Proteger los recursos naturales y los intereses económicos de la Nación.

En ningún caso la información de inteligencia y contrainteligencia será recolectada, procesada o diseminada por razones de género, raza, origen nacional o familiar, lengua, religión, opinión política o filosófica, pertenencia a una organización sindical, social o de derechos humanos, o para promover los intereses de cualquier partido o movimiento político o afectar los derechos y garantías de los partidos políticos de oposición.

ARTÍCULO 5. PRINCIPIOS DE LAS ACTIVIDADES DE INTELIGENCIA Y CONTRAINTELIGENCIA. Quienes autoricen y quienes lleven a cabo actividades de inteligencia y contrainteligencia, además de verificar la relación entre la actividad y los fines enunciados en el artículo 4 de la presente Ley, evaluarán y observarán de manera estricta y en todo momento los siguientes principios:

Principio de necesidad: La actividad de inteligencia y contrainteligencia debe ser necesaria para alcanzar los fines constitucionales deseados; es decir que podrá recurrirse a ésta siempre que no existan otras actividades menos lesivas que permitan alcanzar tales fines.

Principio de idoneidad: La actividad de inteligencia y contrainteligencia debe hacer uso de medios que se adecuen al logro de los fines definidos en el artículo 4 de esta Ley; es decir que se deben usar los medios aptos para el cumplimiento de tales fines y no otros.

Principio de proporcionalidad: La actividad de inteligencia y contrainteligencia deberá ser proporcional a los fines buscados y sus beneficios deben exceder las restricciones impuestas sobre otros principios y valores constitucionales. En particular, los medios y métodos empleados no deben ser desproporcionados frente a los fines que se busca lograr.

ARTÍCULO 6. PROHIBICIÓN DE LA VINCULACIÓN DE MENORES DE EDAD EN ACTIVIDADES DE INTELIGENCIA Y CONTRAINTELIGENCIA. Los organismos de inteligencia y contrainteligencia no podrán en ningún caso vincular a niños, niñas y adolescentes para que lleven a cabo actividades de inteligencia o contrainteligencia.

CAPÍTULO II
REQUERIMIENTOS DE INTELIGENCIA Y CONTRAINTELIGENCIA

ARTÍCULO 7. REQUERIMIENTOS DE INTELIGENCIA Y CONTRAINTELIGENCIA. Los requerimientos definen las áreas y tareas de recolección de información de inteligencia y contrainteligencia de interés prioritario para el Gobierno Nacional.

ARTÍCULO 8. PLAN NACIONAL DE INTELIGENCIA. El Plan Nacional de Inteligencia es el documento de carácter reservado que desarrolla los requerimientos y las prioridades establecidas por el Gobierno Nacional en materia de inteligencia y contrainteligencia, y asigna responsabilidades. Este Plan será elaborado por la Junta de Inteligencia Conjunta y será proyectado para un período de un (1) año. El primer Plan Nacional de Inteligencia entrará en vigencia dentro de los seis (6) meses siguientes a la publicación de la presente Ley.

2

Anexo B. (continuación)

ARTÍCULO 9. REQUERIMIENTOS ADICIONALES. Los requerimientos adicionales a los establecidos en el Plan Nacional de Inteligencia sólo podrán ser determinados por el Presidente de la República, de manera directa o a través del funcionario público que éste designe de manera expresa para ello; el Ministro de Defensa; y, para efectos de cumplir con las funciones de secretario técnico del Consejo de Seguridad Nacional, el Alto Asesor para la Seguridad Nacional. Los demás miembros del Consejo de Seguridad Nacional podrán hacer requerimientos a través de la secretaría técnica del Consejo, que dará trámite para su priorización. Lo anterior, sin perjuicio de los requerimientos que puedan hacer los comandantes de unidades militares y de policía, y los directores de inteligencia para el cumplimiento de su misión constitucional.

CAPÍTULO III
COORDINACIÓN Y COOPERACIÓN EN LAS ACTIVIDADES DE INTELIGENCIA Y CONTRAINTELIGENCIA

ARTÍCULO 10. COORDINACIÓN Y COOPERACIÓN. Los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cooperarán armónica y decididamente, atendiendo los requerimientos de inteligencia y contrainteligencia de los servidores públicos autorizados por esta Ley para efectuarlos, coordinando de manera eficaz y eficiente sus actividades, y evitando la duplicidad de funciones.

ARTÍCULO 11. COOPERACIÓN INTERNACIONAL. Los organismos de inteligencia y contrainteligencia podrán cooperar con organismos de inteligencia homólogos en otros países, para lo cual se establecerán los protocolos de seguridad necesarios para garantizar la protección y reserva de la información, de conformidad con las disposiciones contempladas en la presente Ley.

ARTÍCULO 12. JUNTA DE INTELIGENCIA CONJUNTA (JIC). La Junta de Inteligencia Conjunta se reunirá al menos una vez al mes con el fin de producir estimativos de inteligencia y contrainteligencia para el Gobierno Nacional. Para estos efectos asegurará la cooperación entre los distintos organismos de inteligencia y contrainteligencia. Esta Junta está conformada por:

a. El Ministro de la Defensa Nacional;
b. El Alto Asesor para la Seguridad Nacional, o el funcionario de nivel asesor o superior que delegue para ello el Presidente de la República;
c. El Viceministro de Defensa Nacional;
d. El Jefe de Inteligencia Conjunta, en representación del Comandante General de las Fuerzas Militares;
e. El Jefe de Inteligencia del Ejército Nacional, en representación del Comandante de esa Fuerza;
f. El Jefe de Inteligencia de la Armada Nacional, en representación del Comandante de esa Fuerza;
g. El Jefe de Inteligencia de la Fuerza Aérea Colombiana, en representación del Comandante de esa Fuerza;
h. El Director de Inteligencia Policial, en representación del Director General de la Policía Nacional;
i. El Director de la Unidad de Información y Análisis Financiero (UIAF), o su delegado; y
j. El Director de cualquier otro organismo de inteligencia y contrainteligencia facultado por Ley para llevar a cabo tales actividades.

Parágrafo 1. El Comandante General de las Fuerzas Militares, el Director de la Policía y los Comandantes de Fuerza asistirán a la JIC cuando lo consideren necesario. Los miembros del Consejo de Seguridad Nacional podrán ser invitados a la JIC.

Parágrafo 2. La JIC será presidida por el Ministro de Defensa o por el miembro civil de la JIC que delegue para ello el Presidente de la República.

Parágrafo 3. La participación en la JIC de los organismos que llevan a cabo actividades de inteligencia y contrainteligencia, se dará en el marco de la naturaleza jurídica de la entidad.

Parágrafo 4. Los integrantes de la JIC compartirán la información de inteligencia relevante que tengan a su disposición con los miembros de la misma. En cualquier caso esta información será manejada por los miembros con la debida reserva y observando los protocolos de seguridad de la información.

ARTÍCULO 13. FUNCIONES DE LA JUNTA DE INTELIGENCIA CONJUNTA. La Junta de Inteligencia Conjunta tendrá las siguientes funciones:

a. Elaborar estimativos, informes y/o análisis de inteligencia y contrainteligencia que atiendan los requerimientos y apoyen la toma de decisiones por parte del Gobierno Nacional, en particular en el marco del Consejo de Seguridad Nacional.
b. Elaborar y presentar cada año a consideración del Consejo de Seguridad Nacional para su adopción, el Plan Nacional de Inteligencia de acuerdo con los requerimientos y prioridades establecidos por el Presidente de la República.
c. Coordinar la distribución de tareas para la recolección de información entre los organismos, con el fin de cumplir con las funciones de evaluación y análisis asignadas a la JIC.
d. Establecer, en un término máximo de un (1) año a partir de la vigencia de la presente Ley, los protocolos de intercambio de información entre los organismos de inteligencia y contrainteligencia para garantizar la seguridad y reserva de la información y verificar el cumplimiento de los mismos.
e. Asegurar que existan procedimientos adecuados de protección de la información que sea compartida en la JIC.
f. Suministrar al Consejo de Seguridad Nacional la información de inteligencia y contrainteligencia necesaria para el cumplimiento de sus funciones como máximo órgano asesor del Presidente de la República en asuntos de defensa y seguridad nacional.
g. Hacer seguimiento a la ejecución del Plan Nacional de Inteligencia y elaborar informes periódicos de cumplimiento de las prioridades de inteligencia y contrainteligencia establecidas en el mismo.
h. Presentar a la Comisión Legal de Seguimiento a las Actividades de Inteligencia y Contrainteligencia del Congreso de la República un informe anual que tendrá carácter reservado.
i. Adoptar y modificar su propio reglamento, teniendo en cuenta los fines de la Junta; y

CAPÍTULO IV
CONTROL Y SUPERVISIÓN

ARTÍCULO 14. AUTORIZACIÓN. Las actividades de inteligencia y contrainteligencia deberán ser autorizadas por orden de operaciones o misión de trabajo emitida por los directores de los organismos, o jefes o subjefes de unidad, sección o dependencia, según el equivalente en cada organismo, y deberán incluir un planeamiento.

El nivel de autorización requerido para cada operación o misión de trabajo se incrementará dependiendo de su naturaleza y posible impacto, el tipo de objetivo, el nivel de riesgo para las fuentes o los agentes, y la posible limitación de los derechos fundamentales. Cada organismo definirá, de conformidad con su estructura interna y atendiendo los criterios establecidos en este artículo, quién es el jefe o subjefe de unidad, sección o dependencia encargado de la autorización, en cada caso teniendo en cuenta la Constitución y la Ley.

ARTÍCULO 15. AUTORIZACIÓN DE LAS OPERACIONES DE INTELIGENCIA Y CONTRAINTELIGENCIA. El superior jerárquico en cada caso será responsable de autorizar únicamente aquellas actividades de inteligencia y contrainteligencia que cumplan con los límites y fines enunciados en el artículo 4 de esta Ley, observen los principios del artículo 5 de la misma y estén enmarcadas dentro de un programa de pla-

4

neamiento. Esta autorización deberá obedecer a requerimientos previos de inteligencia o contrainteligencia, de conformidad con el capítulo II de la presente Ley.

Parágrafo. Los funcionarios de los organismos que llevan a cabo actividades de inteligencia y contrainteligencia que infrinjan sus deberes u obligaciones incurrirán en causal de mala conducta, sin perjuicio de la responsabilidad civil, fiscal, penal o profesional que puedan tener. La obediencia debida no podrá ser alegada como eximente de responsabilidad por quien ejecuta la operación de inteligencia cuando ésta suponga una violación a los derechos humanos o una infracción al Derecho Internacional Humanitario – DIH y el Derecho Internacional de los Derechos Humanos.

ARTÍCULO 16. ADECUACIÓN DE MANUALES DE INTELIGENCIA Y CONTRAINTELIGENCIA. Los Directores y Jefes de los organismos de inteligencia y contrainteligencia adecuarán la doctrina de inteligencia y contrainteligencia ajustándola a derecho y derogando aquellas disposiciones que sean contrarias a la Constitución y la presente Ley, en el término máximo de un (1) año contado a partir de la vigencia de la presente ley. Cada organismo de inteligencia establecerá los procedimientos necesarios para revisar la integración de las normas en materia de derechos humanos y derecho internacional humanitario en los manuales de inteligencia y contrainteligencia. Al finalizar este período el Gobierno Nacional deberá presentar un informe sobre la adecuación de los manuales a la Comisión Legal de Seguimiento a las Actividades de Inteligencia y Contrainteligencia del Congreso de la República.

ARTÍCULO 17. MONITOREO DEL ESPECTRO ELECTROMAGNÉTICO E INTERCEPTACIONES DE COMUNICACIONES PRIVADAS. Las actividades de inteligencia y contrainteligencia comprenden actividades de monitoreo del espectro electromagnético debidamente incorporadas dentro de órdenes de operaciones o misiones de trabajo. La información recolectada en el marco del monitoreo del espectro electromagnético en ejercicio de las actividades de inteligencia y contrainteligencia, que no sirva para el cumplimiento de los fines establecidos en la presente Ley, deberá ser destruida y no podrá ser almacenada en las bases de datos de inteligencia y contrainteligencia. El monitoreo no constituye interceptación de comunicaciones.

La interceptación de conversaciones privadas telefónicas móviles o fijas, así como de las comunicaciones privadas de datos, deberán someterse a los requisitos establecidos en el artículo 15 de la Constitución y el Código de Procedimiento Penal y sólo podrán llevarse a cabo en el marco de procedimientos judiciales

ARTÍCULO 18. SUPERVISIÓN Y CONTROL. Los Inspectores de la Policía o la Fuerza Militar a la que pertenezcan los organismos que llevan a cabo actividades de inteligencia y contrainteligencia, deberán rendir un informe anual de carácter reservado tramitado por el conducto regular ante el Ministro de Defensa y con copia a la Comisión Legal de Seguimiento a las Actividades de Inteligencia y Contrainteligencia. Este informe verificará la aplicación de los principios, límites y fines enunciados en esta Ley en la autorización y el desarrollo de actividades de inteligencia y contrainteligencia; la adecuación de la doctrina, los procedimientos y métodos de inteligencia a lo establecido en la presente Ley; así como la verificación de los procesos de actualización, corrección y retiro de datos y archivos de inteligencia y contrainteligencia. Para ello, estos Inspectores contarán con toda la colaboración de los diferentes organismos, quienes en ningún caso podrán revelar sus fuentes y métodos.

Parágrafo 1. En el caso de otros organismos creados por ley para llevar a cabo actividades de inteligencia y contrainteligencia, el informe mencionado deberá ser rendido anualmente por un Inspector o quien haga sus veces ante el Presidente de la República y con copia a la Comisión Legal de Seguimiento a las Actividades de Inteligencia y Contrainteligencia.

Parágrafo 2. En el caso de la Unidad de Información y Análisis Financiero (UIAF), el informe deberá ser rendido anualmente por la Oficina de Control Interno ante el Director, con copia a la Comisión Legal de Seguimiento a las Actividades de Inteligencia y Contrainteligencia.

Parágrafo 3. En cualquier caso el informe rendido por cada entidad no exime al Director de cada organismo de su responsabilidad de velar por el cumplimiento de la presente Ley y demás obligaciones constitucionales y legales. Cualquier incumplimiento a los principios, fines y límites contemplados en la presente Ley deberá ser reportado de inmediato al Presidente de la República, y a las autoridades disciplinarias y judiciales a las que haya lugar.

Parágrafo 4. Los miembros de los organismos de inteligencia y contrainteligencia deberán poner en conocimiento del Jefe o Director del organismo, y en caso de que sea necesario de manera directa ante el Inspector o el Jefe de la Oficina de Control Interno, cualquier irregularidad en el desarrollo de las actividades del organismo. El Director y el Inspector o el Jefe de Control Interno velarán por la protección de la identidad del denunciante.

Parágrafo 5. El Jefe o Director del organismo de inteligencia o contrainteligencia deberá informar anualmente al Presidente de la República sobre las irregularidades en las funciones y actividades de inteligencia y contrainteligencia que se presenten en sus respectivas dependencias.

ARTÍCULO 19. CONTROL POLÍTICO. Se crea la Comisión Legal de Seguimiento a las Actividades de Inteligencia y Contrainteligencia. Modifíquese el artículo 55 de la ley 5ª de 1992 el cual quedará así:

"ARTÍCULO 55. INTEGRACIÓN, DENOMINACIÓN Y FUNCIONAMIENTO. Además de las Comisiones Legales señaladas para cada una de las Cámaras con competencias diferentes a estas corresponderá integrar aplicando el sistema del cociente electoral y para el Periodo Constitucional, la Comisión de Derechos Humanos y Audiencias, la Comisión de Ética y Estatuto del Congresista, la Comisión de Acreditación Documental, la Comisión para la Equidad de la Mujer y la Comisión Legal de Seguimiento a las Actividades de Inteligencia y Contrainteligencia."

ARTICULO 20. OBJETO DE LA COMISIÓN LEGAL DE SEGUIMIENTO A LAS ACTIVIDADES DE INTELIGENCIA Y CONTRAINTELIGENCIA. Adiciónese un artículo 61E a ley 5ª de 1992 el cual quedará así:

"ARTÍCULO 61E. COMISIÓN LEGAL DE SEGUIMIENTO A LAS ACTIVIDADES DE INTELIGENCIA Y CONTRAINTELIGENCIA. Esta comisión, sin perjuicio de las demás facultades otorgadas al Congreso de la República por la Constitución y la Ley, cumplirá funciones de control y seguimiento político, verificando la eficiencia en el uso de los recursos, el respeto de las garantías constitucionales y el cumplimiento de los principios, límites y fines establecidos en la Ley estatutaria que regula las actividades de inteligencia y contrainteligencia."

ARTÍCULO 21 COMPOSICIÓN E INTEGRACIÓN DE LA COMISIÓN LEGAL DE SEGUIMIENTO A LAS ACTIVIDADES DE INTELIGENCIA Y CONTRAINTELIGENCIA. Adiciónese un artículo 61F a ley 5ª de 1992 el cual quedara así:

"ARTÍCULO 61F. COMPOSICIÓN E INTEGRACIÓN. La Comisión Legal de Seguimiento a las Actividades de Inteligencia y Contrainteligencia estará conformada por 8 Congresistas mediante postulación voluntaria, los cuales deberán ser miembros de las Comisiones Segundas Constitucionales Permanentes.

Cada Cámara en Sesión Plenaria, mediante el sistema de cuociente electoral, elegirá cuatro (4) miembros de la respectiva Corporación, garantizando la representación de por lo menos un (1) Representante y un (1) Senador de los partidos y movimientos políticos que se declare : en oposición al Gobierno, salvo que sus voceros de bancada en la Cámara de Representantes y en el Senado de la República, manifiesten ante la Presidencia de la Cámara de Representantes y del Senado de la República respectivamente, de manera libre y expresa su decisión de abstenerse de participar en la Comisión Legal de Seguimiento a las Actividades de Inteligencia y Contrainteligencia.

6

Anexo B. (continuación)

Parágrafo 1. *En caso de que los partidos o movimientos políticos que se declaren en oposición al Gobierno no tengan representación en la Comisión Segunda Constitucional Permanente del Senado o de la Cámara de Representantes, podrá postularse como miembro de la Comisión Legal de Seguimiento de las Actividades de Inteligencia y Contrainteligencia cualquier Senador o Representante a la Cámara que pertenezca a dichos partidos o movimientos políticos.*

Parágrafo 2. *Los partidos o movimientos políticos que se declaren en oposición al Gobierno tendrán derecho a participar al menos uno de ellos, en la mesa directiva de la Comisión Legal de Seguimiento de las Actividades de Inteligencia y Contrainteligencia.*

ARTÍCULO 22. FUNCIONES Y FACULTADES DE LA COMISIÓN LEGAL DE SEGUIMIENTO A LAS ACTIVIDADES DE INTELIGENCIA Y CONTRAINTELIGENCIA. Adiciónese un artículo 61G a la ley 5ª de 1992 el cual quedará así:

"ARTÍCULO 61G. FUNCIONES. Son funciones y facultades de la Comisión Legal de Seguimiento a las Actividades de Inteligencia y Contrainteligencia:

a. *Producir un informe anual reservado dirigido al Presidente de la República, que dé cuenta del cumplimiento de los controles contenidos en la presente Ley y formule recomendaciones para el mejoramiento del ejercicio de las actividades de inteligencia y contrainteligencia, teniendo en cuenta la salvaguarda de la información que afecte la seguridad y la defensa nacional.*
b. *Emitir opiniones y conceptos sobre cualquier proyecto de Ley relacionado con la materia.*
c. *Emitir un concepto sobre el Informe de Auditoría de los gastos reservados elaborado por la Contraloría General de la República.*
d. *Solicitar a la Junta de Inteligencia Conjunta un informe anual de la ejecución general de gastos reservados que dé cuenta del cumplimiento de los objetivos del Plan Nacional de Inteligencia.*
e. *Hacer seguimiento a las recomendaciones incluidas dentro del informe anual del literal a del presente artículo.*
f. *Proponer moción de observación respecto de los Directores de los organismos de inteligencia por asuntos relacionados con funciones propias del cargo o por desatención a los requerimientos y citaciones de la Comisión, o moción de censura a los Ministros del ramo correspondiente.*

Parágrafo 1. *Con el fin de verificar el cumplimiento de los mecanismos de control establecidos en la presente Ley en casos específicos que sean de su interés, la Comisión podrá: (a) realizar reuniones con la JIC; (b) solicitar informes adicionales a los inspectores (incluyendo a los inspectores Ad-hoc designados por los organismos de inteligencia), las Oficinas de Control Interno, o quienes hagan sus veces; (c) citar a los Jefes y Directores de los organismos de inteligencia; (d) conocer los objetivos nacionales de inteligencia trazados en el Plan Nacional de Inteligencia; y (e) conocer los informes presentados anualmente por los inspectores de conformidad con el artículo 18 de la presente ley. Lo anterior sin perjuicio de la reserva necesaria para garantizar la seguridad de las operaciones, las fuentes, los medios y los métodos.*

Parágrafo 2. *En cualquier caso la Comisión pondrá en conocimiento de las autoridades competentes los hechos delictivos o las faltas disciplinarias de las que tenga conocimiento.*

ARTÍCULO 23. ESTUDIOS DE CREDIBILIDAD Y CONFIABILIDAD DE LA COMISIÓN LEGAL DE SEGUIMIENTO A LAS ACTIVIDADES DE INTELIGENCIA Y CONTRAINTELIGENCIA. Adiciónese un artículo 61H a ley 5ª de 1992 el cual quedara así:

ARTÍCULO 61H. Estudios de credibilidad y confiabilidad. Los funcionarios de la Comisión Legal de Seguimiento a las Actividades de Inteligencia y Contrainteligencia, así como los miembros de las unidades de trabajo legislativo que sean designados por cada miembro de la Comisión para apoyar el trabajo de la misma, se someterán a por lo

menos un (1) estudio de credibilidad y confianza al año. Las mesas directivas del Senado y la Cámara de Representantes determinarán el organismo de la comunidad de inteligencia a través del cual se aplicarán los estudios y reglamentarán los procedimientos necesarios para garantizar la reserva de los resultados de estos estudios.

Las mesas Directivas de Senado y Cámara diseñarán conjuntamente los criterios y parámetros a tener en cuenta para la evaluación y calificación de los estudios de credibilidad y confiabilidad, así como los protocolos necesarios para garantizar la absoluta reserva de la información relacionada con tales estudios.

ARTÍCULO 24. DEBER DE RESERVA DE LA COMISIÓN. Los miembros de la Comisión Legal de Seguimiento a las Actividades de Inteligencia y Contrainteligencia están obligados a guardar reserva sobre las informaciones y documentos a los que tengan acceso durante y después de su membrecía, hasta el término que establece la presente Ley.

Parágrafo 1. Ningún documento público emanado de la Comisión podrá revelar datos que puedan perjudicar la función de inteligencia; poner en riesgo las fuentes, los medios o los métodos; o atentar contra la vigencia del régimen democrático, la seguridad o la defensa nacional.

Parágrafo 2. Los miembros de la Comisión así como el personal permanente o eventual asignado a la misma que hicieran uso indebido de la información a la que tuvieren acceso en ocasión o ejercicio de sus funciones, en los términos de la Ley, serán considerados incursos en causal de mala conducta sin perjuicio de la responsabilidad penal a que haya lugar y quedarán inhabilitados para ser miembros de la Comisión Legal de Seguimiento a las Actividades de Inteligencia y Contrainteligencia.

ARTÍCULO 25. FUNCIONAMIENTO. Las mesas directivas del Senado y la Cámara de Representantes asignarán los recursos humanos y físicos necesarios para el funcionamiento de la Comisión Legal de Seguimiento a las Actividades de Inteligencia y Contrainteligencia. La Comisión podrá solicitar a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia la designación de enlaces permanentes para el cumplimiento de sus funciones.

ARTÍCULO 26. PLANTA DE PERSONAL DE LA COMISIÓN LEGAL DE SEGUIMIENTO A LAS ACTIVIDADES DE INTELIGENCIA Y CONTRAINTELIGENCIA. Adiciónese al artículo 389 de la Ley 5 de 1992 el numeral 2.6.13, así:

"2.6.13 Comisión Legal de Seguimiento a las actividades de Inteligencia y Contrainteligencia.

CANTIDAD	CARGO
1	Secretario de Comisión
1	Asesor
1	Transcriptor

El grado y la remuneración de cada funcionario será el mismo que el de los funcionarios del mismo cargo en las Comisiones Constitucionales.

***Parágrafo.** En todo caso, el Secretario de Comisión, previa solicitud a la dirección administrativa de Senado o Cámara, según sea el caso, adecuará el personal necesario para el correcto funcionamiento de la Comisión únicamente con personal de planta.*

ARTÍCULO 27. DEBATES EN MATERIA DE INTELIGENCIA Y CONTRAINTELIGENCIA. Adiciónese el artículo 94 de la ley 5 de 1992 así:

ARTÍCULO 94. DEBATES. El sometimiento a discusión de cualquier proposición o proyecto sobre cuya adopción deba resolver la respectiva Corporación, es lo que constituye el debate. El debate empieza al abrirlo el Presidente y termina con la votación general. Los debates en materia de inteligencia y contrainteligencia se adelantarán en sesión reservada.

CAPÍTULO V
BASES DE DATOS Y ARCHIVOS DE INTELIGENCIA Y CONTRAINTELIGENCIA

ARTÍCULO 28. CENTROS DE PROTECCIÓN DE DATOS DE INTELIGENCIA Y CONTRAINTELIGENCIA. Cada uno de los organismos que desarrolla actividades de inteligencia y contrainteligencia tendrá un Centro de Protección de datos y archivos de Inteligencia y Contrainteligencia (CPD). Cada Centro tendrá un responsable que garantizará que los procesos de recolección, almacenamiento, producción y difusión de la información de inteligencia y contrainteligencia estén enmarcados en la Constitución y la Ley. Para ello se llevarán a cabo los talleres de capacitación necesarios dentro de cada organismo.

ARTÍCULO 29. OBJETIVOS DE LOS CENTROS DE PROTECCIÓN DE DATOS DE INTELIGENCIA Y CONTRAINTELIGENCIA (CPD). Cada CPD tendrá los siguientes objetivos:

a. Controlar el ingreso y la salida de información a las bases de datos y archivos de inteligencia y contrainteligencia, garantizando de manera prioritaria su reserva constitucional y legal.
b. Asegurar que aquellos datos de inteligencia y contrainteligencia que una vez almacenados no sirvan para los fines establecidos en el artículo 5 de la presente Ley, sean retirados.
c. Garantizar que la información no será almacenada en las bases de datos de inteligencia y contrainteligencia por razones de género, raza, origen nacional o familiar, lengua, religión, opinión política o filosófica, pertenencia a una organización sindical, social o de derechos humanos, o para promover los intereses de cualquier partido o movimiento político o afectar los derechos y garantías de los partidos políticos de oposición.

ARTÍCULO 30. COMISIÓN ASESORA PARA LA DEPURACIÓN DE DATOS Y ARCHIVOS DE INTELIGENCIA Y CONTRAINTELIGENCIA. Créase la Comisión asesora para la depuración de los datos y archivos de inteligencia y contrainteligencia que será presidida por el Procurador General de la Nación. Esta Comisión estará integrada por un (1) miembro designado por el Presidente de la República; un (1) miembro del Grupo de Memoria Histórica de la Comisión Nacional de Reparación y Reconciliación o quien haga sus veces; un (1) integrante de los organismos que llevan a cabo actividades de inteligencia y contrainteligencia; un (1) representante de la Comisión Legal de Seguimiento a las Actividades de Inteligencia y Contrainteligencia; un (1) académico nacional o internacional experto en temas de inteligencia; un (1) representante de la sociedad civil; y un (1) delegado de la Defensoría del Pueblo.

Esta Comisión tendrá una vigencia de dos (2) años a partir de su conformación. Su objeto será producir un Informe en el que se formulen recomendaciones al Gobierno Nacional sobre los criterios de permanencia, los criterios de retiro, y el destino de los datos y archivos de inteligencia y contrainteligencia que sean retirados. Para ello la Comisión tendrá en cuenta las siguientes consideraciones: a) la seguridad nacional; b) los derechos fundamentales de los ciudadanos al buen nombre, la honra y el debido proceso; c) el deber de garantizar la preservación de la memoria histórica de la Nación; d) la protección de la información, de los servidores públicos que desarrollan actividades de inteligencia y contrainteligencia, y de las fuentes, medios y métodos; e) la Ley de archivos; f) los artículos 4 y 5 de la presente Ley; y g) las prácticas internacionales sobre depuración de datos y archivos de inteligencia. La Comisión podrá solicitar asesoría técnica externa para el cumplimiento de su función, y entregar informes parciales antes del vencimiento de su mandato.

9

Anexo B. (continuación)

El Gobierno Nacional pondrá en marcha, dentro del año siguiente a la rendición del informe de la Comisión, un sistema de depuración de datos y archivos de inteligencia y contrainteligencia, orientado por el informe de recomendaciones de la Comisión.

Una vez creado el sistema de depuración de datos y archivos de inteligencia y contrainteligencia, el Gobierno Nacional rendirá informes periódicos a la Procuraduría General de la Nación sobre la implementación del mismo.

ARTÍCULO 31. COMITÉS DE ACTUALIZACIÓN, CORRECCIÓN Y RETIRO DE DATOS Y ARCHIVOS DE INTELIGENCIA. Cada organismo de inteligencia creará un comité para la corrección, actualización y retiro de datos e información de inteligencia de conformidad con los principios, límites y fines establecidos en la presente Ley. La información que haya sido recaudada para fines distintos de los establecidos en el artículo 4 de la presente Ley, o por las razones establecidas en el último inciso del mismo artículo, será retirada de las bases de datos y archivos de inteligencia, y almacenada en un archivo histórico hasta tanto la Comisión para la depuración rinda su informe de recomendaciones.

ARTÍCULO 32. SUPERVISIÓN Y CONTROL. El informe anual de los Inspectores de Fuerza y las Oficinas de control interno, o quienes hagan sus veces, contemplado en el artículo 18 de la presente Ley deberá incluir la verificación del cumplimiento de los procesos de actualización, corrección y retiro de datos y archivos de inteligencia y contrainteligencia.

CAPÍTULO VI
RESERVA DE LA INFORMACIÓN DE INTELIGENCIA Y CONTRAINTELIGENCIA

ARTÍCULO 33. RESERVA. Por la naturaleza de las funciones que cumplen los organismos de inteligencia y contrainteligencia sus documentos, información y elementos técnicos estarán amparados por la reserva legal por un término máximo de treinta (30) años contados a partir de la recolección de la información y tendrán carácter de información reservada.

Excepcionalmente y en casos específicos, por recomendación de cualquier organismo que lleve a cabo actividades de inteligencia y contrainteligencia, el Presidente de la República podrá acoger la recomendación de extender la reserva por quince (15) años más, cuando su difusión suponga una amenaza grave interna o externa contra la seguridad o la defensa nacional, se trate de información que ponga en riesgo las relaciones internacionales, esté relacionada con grupos armados al margen de la ley, o atente contra la integridad personal de los agentes o las fuentes.

Parágrafo 1. El Presidente de la República podrá autorizar en cualquier momento, antes del cumplimiento del término de la reserva, la desclasificación total o parcial de los documentos cuando considere que el levantamiento de la reserva contribuirá al interés general y no constituirá una amenaza contra la vigencia del régimen democrático, la seguridad, o defensa nacional, ni la integridad de los medios, métodos y fuentes.

Parágrafo 2. El organismo de inteligencia que decida ampararse en la reserva para no suministrar una información que tenga este carácter, debe hacerlo por escrito, y por intermedio de su director, quien motivará por escrito la razonabilidad y proporcionalidad de su decisión y la fundará en esta disposición legal. En cualquier caso, frente a tales decisiones procederán los recursos y acciones legales y constitucionales del caso.

Parágrafo 3. El servidor público que tenga conocimiento sobre la recolección ilegal de información de inteligencia y contrainteligencia, la pondrá en conocimiento de las autoridades administrativas, penales y disciplinarias a las que haya lugar, sin que ello constituya una violación a la reserva.

10

Anexo B. (continuación)

Parágrafo 4. El mandato de reserva no vincula a los periodistas ni a los medios de comunicación cuando ejerzan su función periodística de control del poder público, en el marco de la autorregulación periodística y la jurisprudencia constitucional, quienes en cualquier caso estarán obligados a garantizar la reserva respecto de sus fuentes.

ARTÍCULO 34. INOPONIBILIDAD DE LA RESERVA. El carácter reservado de los documentos de inteligencia y contrainteligencia no será oponible a las autoridades judiciales, disciplinarias y fiscales que lo soliciten para el debido ejercicio de sus funciones, siempre que su difusión no ponga en riesgo la seguridad o la defensa nacional, ni la integridad personal de los ciudadanos, los agentes, o las fuentes. Corresponderá a dichas autoridades asegurar la reserva de los documentos que lleguen a conocer en desarrollo de lo establecido en el presente artículo.

Parágrafo. Salvo lo dispuesto en el parágrafo 4 del artículo 12 de la presente Ley, la inoponibilidad de la reserva en el caso de la UIAF estará regulada de manera especial por el inciso 4 del artículo 9 de la Ley 526 de 1999, el cual quedará así: "La información que recaude la UIAF en cumplimiento de sus funciones y la que se produzca como resultado de su análisis estará sujeta a reserva, salvo que medie solicitud de las fiscalías con expresas funciones legales para investigar lavado de activos o sus delitos fuente, financiación del terrorismo y/o legitimadas para ejercitar la acción de extinción de dominio quienes deberán mantener la reserva aquí prevista."

ARTÍCULO 35. VALOR PROBATORIO DE LOS INFORMES DE INTELIGENCIA. En ningún caso los informes de inteligencia y contrainteligencia tendrán valor probatorio dentro de procesos judiciales y disciplinarios, pero su contenido podrá constituir criterio orientador durante la indagación. En todo caso se garantizará la reserva de la información, medios, métodos y fuentes, así como la protección de la identidad de los funcionarios de inteligencia y contrainteligencia.

ARTÍCULO 36. RECEPTORES DE PRODUCTOS DE INTELIGENCIA Y CONTRAINTELIGENCIA. Podrán recibir productos de inteligencia y contrainteligencia, de conformidad con las reglas de reserva establecidas en los artículos 33 y 38 de la presente Ley:

a. El Presidente de la República;
b. Los miembros del Consejo de Seguridad Nacional y, en lo relacionado con las sesiones a las que asistan, los invitados al Consejo de Seguridad Nacional;
c. El Secretario General de la Presidencia de la República, los Ministros y Viceministros, y el Secretario Privado del Presidente de la República en lo relacionado con el cumplimiento de sus funciones;
d. Los miembros de la Comisión Legal de Inteligencia y Contrainteligencia;
e. Los miembros de la Fuerza Pública de acuerdo con sus funciones y niveles de acceso a la información;
f. Los demás servidores públicos de acuerdo con sus funciones y niveles de acceso a la información de conformidad con el artículo 37 de la presente Ley, y siempre que aprueben los exámenes de credibilidad y confiabilidad establecidos para ello; y
g. Los organismos de inteligencia de otros países con los que existan programas de cooperación.

Parágrafo 1. Los Jefes y Directores de los organismos de inteligencia y contrainteligencia establecerán los procedimientos y controles para la difusión y trazabilidad de la información de inteligencia y contrainteligencia. La difusión deberá hacerse en el marco de los fines, límites y principios establecidos en el marco de la presente Ley.

Parágrafo 2. Los asesores externos y contratistas sólo podrán recibir información de inteligencia y contrainteligencia de acuerdo con el nivel de acceso a la información que le haya sido asignado de conformidad con el artículo 37 de la presente Ley, dentro del objeto de su asesoría o contrato, y previo estudio de credibilidad y confiabilidad.

11

Anexo B. (continuación)

ARTÍCULO 37. NIVELES DE CLASIFICACIÓN. El Gobierno Nacional, dentro del año siguiente a la publicación de la presente Ley, reglamentará los niveles de clasificación de la información y diseñará un sistema para la designación de los niveles de acceso a la misma por parte de los servidores públicos.

ARTÍCULO 38. COMPROMISO DE RESERVA. Los servidores públicos de los organismos que desarrollen actividades de inteligencia y contrainteligencia, los funcionarios que adelanten actividades de control, supervisión y revisión de documentos o bases de datos de inteligencia y contrainteligencia, y los receptores de productos de inteligencia, se encuentran obligados a suscribir acta de compromiso de reserva en relación con la información de que tengan conocimiento. Quienes indebidamente divulguen, entreguen, filtren, comercialicen, empleen o permitan que alguien emplee la información o documentos reservados, incurrirán en causal de mala conducta, sin perjuicio de las acciones penales a que haya lugar.

Para garantizar la reserva, los organismos de inteligencia y contrainteligencia podrán aplicar todas las pruebas técnicas, con la periodicidad que consideren conveniente, para la verificación de las calidades y el cumplimiento de los más altos estándares en materia de seguridad por parte de los servidores públicos que llevan a cabo actividades de inteligencia y contrainteligencia.

Parágrafo 1. El deber de reserva de los servidores públicos de los organismos que desarrollen actividades de inteligencia y contrainteligencia, y de receptores antes mencionados, permanecerá aún después del cese de sus funciones o retiro de la institución hasta el término máximo que establece la presente Ley.

Parágrafo 2. Los organismos que desarrollan actividades de inteligencia y contrainteligencia deberán tomar todas las medidas necesarias para impedir que sus miembros copien, porten, reproduzcan, almacenen, manipulen o divulguen cualquier tipo de información de inteligencia o contrainteligencia con fines distintos al cumplimiento de su misión.

Parágrafo 3. Las personas capacitadas para cumplir funciones relacionadas con las actividades de inteligencia y contrainteligencia, deberán cumplir en todo momento los más altos estándares de idoneidad y confianza que permitan mantener el compromiso de reserva en el desarrollo de sus funciones. Para tal efecto cada una de las entidades que realizan actividades de inteligencia y contrainteligencia, desarrollarán protocolos internos para el proceso de selección, contratación, incorporación y capacitación del personal de inteligencia y contrainteligencia, teniendo en cuenta la doctrina, funciones y especialidades de cada una de las entidades.

Parágrafo 4. La no superación de las pruebas de credibilidad y confiabilidad será causal de no ingreso o retiro del organismo de inteligencia y contrainteligencia de acuerdo con la reglamentación establecida por el Gobierno Nacional. En los organismos de inteligencia y contrainteligencia que no pertenezcan al sector defensa, el retiro del servicio de los servidores públicos que llevan a cabo actividades de inteligencia y contrainteligencia se producirá cuando el nominador, previo concepto de un comité asesor o quien haga sus veces, en ejercicio de la facultad discrecional considere que no se cumplen con los estándares de idoneidad y confianza.

Para los organismos de inteligencia y contrainteligencia que pertenecen al sector defensa, el retiro de servicios se hará de conformidad con las normas de carrera correspondientes.

ARTÍCULO 39. EXCEPCIÓN A LOS DEBERES DE DENUNCIA Y DECLARACIÓN. Los servidores públicos de los organismos que desarrollan actividades de inteligencia y contrainteligencia están obligados a guardar la reserva en todo aquello que por razón del ejercicio de sus actividades hayan visto, oído o comprendido. En este sentido, los servidores públicos a los que se refiere este artículo están exonerados del deber de denuncia y no podrán ser obligados a declarar. Lo anterior sin perjuicio de lo establecido en los parágrafos 3 y 4 del artículo 18 y del parágrafo 3 del artículo 33.

12

La exclusión del deber de denuncia no aplicará para los casos en que el servidor público posea información relacionada con la presunta comisión de genocidio, ejecuciones extrajudiciales, tortura, desplazamiento forzado, desaparición forzada, violencia sexual masiva, crímenes de lesa humanidad, o crímenes de guerra por parte de un servidor público.

En cualquier caso los servidores públicos de los organismos que desarrollan actividades de inteligencia y contrainteligencia podrán denunciar las actividades delictivas de las que tengan conocimiento de manera directa o mediante representante del organismo de inteligencia y en condiciones que permitan garantizar su seguridad e integridad, garantizando la protección de fuentes, medios y métodos.

En caso de que el organismo considere necesario declarar en un proceso podrá hacerlo a través del Director o su delegado.

Cuando los servidores públicos a que se refiere este artículo deban denunciar o rendir testimonio, el juez o el fiscal según el caso, podrán disponer que la diligencia respectiva se reciba en forma privada y se mantenga en reserva mientras ello sea necesario para asegurar la vida e integridad personal del funcionario y la de su familia.

CAPÍTULO VII
PROTECCIÓN DE LOS SERVIDORES PÚBLICOS QUE REALIZAN ACTIVIDADES DE INTELIGENCIA Y CONTRAINTELIGENCIA

ARTÍCULO 40. PROTECCIÓN DE LA IDENTIDAD. Con el fin de proteger la vida e integridad de los servidores públicos que desarrollan actividades de inteligencia y contrainteligencia, y para facilitar la realización de las actividades propias de su cargo, el gobierno a través de la Registraduría Nacional del Estado Civil, les suministrará documentos con nueva identidad que deberán ser utilizados exclusivamente en el ejercicio de sus funciones y actividades.

Los Jefes y Directores de los organismos de inteligencia serán los únicos autorizados para solicitar ante la Registraduría Nacional del Estado Civil la expedición del nuevo documento de identificación para la protección de sus funcionarios, sin perjuicio de la responsabilidad penal, disciplinaria y fiscal por la omisión de denuncia del uso indebido, y el incumplimiento al debido control del uso de los documentos expedidos.

En caso de necesitarse la expedición de otros documentos públicos o privados para el cumplimiento de la misión, los funcionarios de los organismos que llevan a cabo actividades de inteligencia y contrainteligencia podrán utilizar para el trámite el nuevo documento de identidad expedido por la Registraduría Nacional del Estado Civil, sin que el uso de los nuevos documentos constituya infracción a la Ley.

La Registraduría Nacional del Estado Civil con el apoyo de los organismos de inteligencia y contrainteligencia, reglamentarán la implementación del sistema de custodia de la información relacionada con la identidad funcional de los agentes con el fin de garantizar la seguridad de la información y la protección de la vida e integridad física de los agentes.

Los organismos de inteligencia serán responsables de garantizar la reserva de esta información de acuerdo con lo establecido en la presente Ley.

Parágrafo 1. En la implementación de los mecanismos de protección contemplados en este artículo, las entidades estatales deberán suscribir los convenios interinstitucionales a que haya lugar con el fin de establecer protocolos para asegurar la reserva, seguridad y protección de la información.

13

Parágrafo 2. El servidor público que indebidamente dé a conocer información sobre la identidad de quienes desarrollen actividades de inteligencia o contrainteligencia incurrirá en causal de mala conducta, sin perjuicio de las acciones penales a que haya lugar.

Parágrafo 3. El uso indebido de los documentos de identidad a los que se refiere el presente artículo será causal de mala conducta sin perjuicio de las acciones penales a las que haya lugar.

ARTÍCULO 41. PROTECCIÓN DE LOS SERVIDORES PÚBLICOS QUE DESARROLLAN ACTIVIDADES DE INTELIGENCIA Y CONTRAINTELIGENCIA Y SU NÚCLEO FAMILIAR. Los servidores públicos pertenecientes a los organismos que desarrollan actividades de inteligencia y contrainteligencia que con ocasión del cumplimiento de sus funciones y actividades se vean compelidos a riesgo o amenaza actual e inminente contra su integridad personal o la de su núcleo familiar, tendrán la debida protección del Estado. Para este propósito cada institución establecerá los mecanismos de protección pertinentes.

CAPÍTULO VIII
DEBERES DE COLABORACIÓN DE LAS ENTIDADES PÚBLICAS Y PRIVADAS

ARTÍCULO 42. COLABORACIÓN DE LAS ENTIDADES PÚBLICAS Y PRIVADAS. Los organismos de inteligencia podrán solicitar la cooperación de las entidades públicas y privadas para el cumplimiento de los fines enunciados en esta Ley. En caso de que la información solicitada por el organismo de inteligencia esté amparada por la reserva legal, estos organismos y las entidades públicas y privadas podrán suscribir convenios interinstitucionales de mutuo acuerdo. En cualquier caso, la entrega de tal información no constituirá una violación a la reserva legal, toda vez que la misma continuará bajo este principio, al cual se encuentran obligados los servidores públicos de inteligencia y contrainteligencia en virtud de lo dispuesto en la presente Ley.

ARTÍCULO 43. COLABORACIÓN CON AUTORIDADES DE POLICÍA JUDICIAL. Los Fiscales, en casos específicos, podrán entregar a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia copias de los documentos y medios técnicos recaudados como elementos materiales probatorios cuando ello sea necesario para el cumplimiento de los fines establecidos en el artículo 4 de la presente Ley, sin que ello implique una violación de la cadena de custodia. Lo anterior previa solicitud del director del organismo de inteligencia o su delegado. En todo caso los organismos de inteligencia y contrainteligencia quedarán obligados a garantizar la reserva de tales documentos.

ARTÍCULO 44. COLABORACIÓN CON OPERADORES DE SERVICIOS DE TELECOMUNICACIONES. Los operadores de servicios de telecomunicaciones estarán obligados a suministrar a los organismos de inteligencia y contrainteligencia, previa solicitud y en desarrollo de una operación autorizada y siempre que sea técnicamente viable, el historial de comunicaciones de los abonados telefónicos vinculados, los datos técnicos de identificación de los suscriptores sobre los que recae la operación, así como la localización de las celdas en que se encuentran las terminales y cualquier otra información que contribuya a su localización. Los organismos de inteligencia y contrainteligencia garantizarán la seguridad de esta información y con tal fin, en la solicitud que formulen a los operadores de servicios de telecomunicaciones, limitarán la información solicitada a un periodo que no exceda de cinco (5) años.

Los Directores de los organismos de inteligencia, o quienes ellos deleguen, serán los encargados de presentar por escrito a los operadores de servicios de telecomunicaciones la solicitud de dicha información.
En todo caso, la interceptación de comunicaciones estará sujeta a los procedimientos establecidos por el artículo 15 de la Constitución y el Código de Procedimiento Penal y sólo podrá llevarse a cabo en el marco de procesos judiciales.

14

Anexo B. (continuación)

Parágrafo 1. Los operadores de servicios de telecomunicaciones deberán informar al Ministerio de Tecnologías de la Información y Comunicaciones y a la Fiscalía General de la Nación cualquier modificación en la tecnología de sus redes que tenga incidencia sobre la interceptación de comunicaciones y poner a su disposición, en un tiempo y a un costo más una utilidad razonable, la implementación de los equipos de interceptación para la adaptación a la red. La información suministrada será reservada. Los operadores de servicios de telecomunicaciones deberán indicar el contenido y el alcance de la modificación respectiva con una antelación no inferior a 60 días calendario a aquél en que se pretenda llevar a cabo la misma.

Parágrafo 2. Los operadores de servicios de telecomunicaciones deberán ofrecer a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia, un medio de transporte que permita llamadas de voz encriptadas, a un costo más una utilidad razonable, y para un número específico de usuarios en condiciones que no degraden la red del operador ni la calidad del servicio que éste presta. Este medio se otorgará a solicitud de la Junta de Inteligencia Conjunta; será exclusivo del alto gobierno y de los organismos de inteligencia y contrainteligencia del Estado; y será regulado y controlado por la Junta de Inteligencia Conjunta.

Parágrafo 3. Los proveedores de redes y/o servicios de telecomunicaciones bajo ninguna circunstancia serán responsables de la utilización que se haga de la información de los usuarios que sea suministrada a los organismos de inteligencia y contrainteligencia del Estado en cumplimiento de las anteriores disposiciones.

CAPÍTULO IX
DISPOSICIONES DE VIGENCIA

ARTÍCULO 45. DEROGATORIAS. La presente Ley deroga todas las disposiciones que le sean contrarias, en especial el Decreto 2233 de 1995 "Por medio del cual se crean el Sistema Nacional de Inteligencia, el Consejo Técnico Nacional de Inteligencia, los Consejos Técnicos Seccionales de Inteligencia..." y el decreto 324 de 2000 "por el cual se crea el Centro de coordinación de la lucha contra los grupos de autodefensas ilegales y demás grupos al margen de la Ley".

ARTÍCULO 46. VIGENCIA. La presente Ley rige a partir de la fecha de su publicación.

EL PRESIDENTE DEL HONORABLE SENADO DE LA REPÚBLICA

ROY LEONARDO BARRERAS MONTEALEGRE

EL SECRETARIO GENERAL DEL HONORABLE SENADO DE LA REPUBLICA

GREGORIO ELJACH PACHECO

15

Anexo B. (continuación)

EL PRESIDENTE DE LA HONORABLE CAMARA DE REPRESENTANTES

AUGUSTO POSADA SANCHEZ

EL SECRETARIO GENERAL DE LA HONORABLE CAMARA DE REPRESENTANTES

JORGE HUMBERTO MANTILLA SERRANO

16

Anexo B. (continuación)

LEY ESTATUTARIA No. 1621

"POR MEDIO DEL CUAL SE EXPIDEN NORMAS PARA FORTALECE EL MARCO JURÍDICO QUE PERMITE A LOS ORGANISMOS QUE LLEVAN A CABO ACTIVIDADES DE INTELIGENCIA Y CONTRAINTELIGENCIA CUMPLIR CON SU MISIÓN CONSTITUCIONAL Y LEGAL, Y SE DICTAN OTRAS DISPOSICIONES"

REPÚBLICA DE COLOMBIA - GOBIERNO NACIONAL

PUBLÍQUESE Y CÚMPLASE

En cumplimiento de lo dispuesto en la Sentencia C-540 de fecha 12 de julio de dos mil doce (2012) – Radicación: PE-033, proferida por la H. Corte Constitucional, se procede a la sanción del proyecto de Ley, la cual ordena la remisión del expediente al Congreso de la República, para continuar el trámite de rigor y posterior envío al Presidente de la República.

Dada en Bogotá, D.C., a los 17 ABR 2013

LA MINISTRA DE JUSTICIA Y DEL DERECHO,

RUTH STELLA CORREA PALACIO

EL MINISTRO DE DEFENSA NACIONAL,

JUAN CARLOS PINZÓN BUENO

EL DIRECTOR DEL DEPARTAMENTO ADMINISTRATIVO – DIRECCIÓN NACIONAL DE INTELIGENCIA,

ALVARO ECHANDÍA DURÁN

SECRETARIA JURIDICA

Recibió: _____

Hora: _____

REPÚBLICA DE COLOMBIA

MINISTERIO DE DEFENSA NACIONAL

DECRETO NÚMERO -857 DE 2014

(2 MAY 2014

"Por el cual se reglamenta la Ley Estatutaria 1621 del 17 de abril de 2013, "Por medio de la cual se expiden normas para fortalecer el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, cumplir con su misión constitucional y legal, y se dictan otras disposiciones".

EL PRESIDENTE DE LA REPÚBLICA DE COLOMBIA

En ejercicio de las facultades constitucionales y legales, en especial la que confiere el numeral 11 del artículo 189 de la Constitución Política, y

CONSIDERANDO:

Que la Ley Estatutaria 1621 del 17 de abril de 2013, contiene normas para fortalecer el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, cumplir con su misión constitucional y legal, siendo necesaria la reglamentación de algunos de sus artículos para efectos de su adecuada, armoniosa, eficaz y eficiente ejecución.

Que el presente decreto reglamenta parcialmente la ley 1621 del 17 de abril de 2013.

DECRETA:

CAPITULO I

Delimitación de los Organismos, dependencias y personal que realizan actividades de inteligencia y contrainteligencia

Artículo 1. Delimitación de los Organismos y dependencias. Llevarán a cabo actividades de inteligencia y contrainteligencia los organismos y dependencias autorizados por la ley. Estos organismos y las dependencias autorizadas desarrollaran estas actividades observando la Constitución y la Ley y serán los siguientes:

1. En las Fuerzas Militares:

a. En el Comando General de las Fuerzas Militares:

1. La Jefatura de Inteligencia y Contrainteligencia Militar Conjunta, sus Direcciones, Divisiones y/o equivalentes y demás unidades o dependencias de inteligencia y contrainteligencia subordinadas a ella.

2. Las unidades o dependencias de inteligencia y contrainteligencia en cada uno de los Comandos Conjuntos o Comandos de Fuerza de Tarea Conjunta.

3. Las unidades o dependencias especiales creadas por el Comandante General de las Fuerzas Militares, mediante acto administrativo, para realizar actividades de Inteligencia y Contrainteligencia, previo concepto de la Jefatura de Inteligencia y Contrainteligencia Militar Conjunta, de acuerdo con su misión, competencias y funciones.

b. En el Ejército Nacional:

1. La Jefatura de Inteligencia y Contrainteligencia del Ejército Nacional, las dependencias y unidades de Inteligencia y contrainteligencia subordinadas a ella.

2. Las dependencias de inteligencia y contrainteligencia en cada División, Brigada, Batallón y unidades que por su naturaleza y misión desarrollen estas actividades en sus diferentes niveles.

3. Las unidades especiales creadas por el Comandante del Ejército, mediante acto administrativo, para realizar actividades de Inteligencia y Contrainteligencia, previo concepto de la Jefatura de Inteligencia y Contrainteligencia Militar, de acuerdo con su misión, competencias y funciones.

Vo.Bo.: DIRECTOR ASUNTOS LEGALES
Vo.Bo.: COORDINADORA GRUPO NEGOCIOS GENERALES

Anexo C. (continuación)

c. En la Armada Nacional:

1. La Jefatura de Inteligencia Naval, las dependencias y unidades de inteligencia y contrainteligencia subordinadas a ella.

2. Las dependencias de inteligencia y contrainteligencia en cada una de las unidades de la Armada Nacional, que por su naturaleza, misión y organización desarrollen estas actividades en sus diferentes niveles.

3. Las unidades especiales creadas por el Comandante de la Armada Nacional, mediante acto administrativo, para realizar actividades de Inteligencia y Contrainteligencia, previo concepto de la Jefatura de Inteligencia Naval, de acuerdo con su misión, competencias y funciones.

d. En la Fuerza Aérea Colombiana:

1. La Jefatura de Inteligencia Aérea, las dependencias y unidades de inteligencia y contrainteligencia subordinadas a ella.

2. Las dependencias de inteligencia y contrainteligencia en cada una de las unidades de la Fuerza Aérea Colombiana, a nivel estratégico, operacional y táctico, que por su naturaleza y misión desarrollen estas actividades en sus diferentes niveles.

3. Las unidades especiales autorizadas por el Comandante de la Fuerza Aérea Colombiana, mediante acto administrativo, para realizar actividades de Inteligencia y Contrainteligencia, previo concepto de la Jefatura de Inteligencia Aérea, de acuerdo con su misión, competencias y funciones.

2. En la Policía Nacional:

a. La Dirección de Inteligencia Policial con sus dependencias subordinadas, la cual dirigirá, coordinará e integrará la función de inteligencia y contrainteligencia en la Policía Nacional.

b. Los grupos especializados de la Policía Nacional que sean creados por el Director General de la Policía Nacional, previo concepto de la Dirección de Inteligencia Policial, de acuerdo con su misión, competencias y funciones.

3. En el Departamento Administrativo "Dirección Nacional de Inteligencia"

Todas las dependencias orgánicas a ella.

4. En la Unidad de Información y Análisis Financiero - UIAF

Todas las dependencias orgánicas a ella.

CAPITULO II

Requerimientos de Inteligencia y Contrainteligencia

Artículo 2. Plan Nacional de Inteligencia. El Plan Nacional de Inteligencia, es el documento que desarrolla los requerimientos y las prioridades establecidas por el Gobierno Nacional en materia de inteligencia y contrainteligencia, y asigna responsabilidades, deberá contener como mínimo los siguientes elementos estructurales en su elaboración y adopción:

a. **Objetivo General.** En este punto se indicarán los aspectos ordenados por la Constitución y la ley para la elaboración del Plan Nacional de Inteligencia.

b. **Límites y fines.** El Plan Nacional de Inteligencia, se ajustará a lo dispuesto en los artículos 4 y 5 de la Ley 1621 de 2013.

Vo.Bo.: DIRECTOR ASUNTOS LEGALES
Vo.Bo. COORDINADORA GRUPO NEGOCIOS GENERALES
Revisó: MY. VÍCTOR HUGO PEÑA JIMÉNEZ

Continuación del Decreto. "Por el cual se reglamenta la Ley Estatutaria 1621 del 17 de abril de 2013, "Por medio de la cual se expiden normas para fortalecer el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, cumplir con su misión constitucional y legal, y se dictan otras disposiciones".

c. **Requerimientos.** Son aquellos determinados en los artículos 7 y 9 de la Ley 1621 de 2013.

d. **Amenazas, riesgos, prioridades.** El Plan Nacional de Inteligencia debe orientar la coordinación, cooperación y esfuerzo relacionados con el desarrollo de la función y las actividades de inteligencia y contrainteligencia, frente a posibles amenazas y riesgos contra la seguridad y defensa nacional y demás fines enunciados en la Ley 1621 de 2013, observando las potencialidades y capacidades del Estado, dando prioridad en su ejecución a aquellas actividades de inteligencia y contrainteligencia que el Gobierno Nacional requiera, bien sea por su impacto, probabilidad de ocurrencia, valor estratégico y/o afectación de los intereses nacionales.

e. **Asignación de responsabilidades. La asignación de responsabilidades en el Plan debe estar** alineada con la misión constitucional y legal, y ser conforme a las competencias y al principio de especialidad de cada uno de los organismos que desarrollan actividades de inteligencia y contrainteligencia.

f. **Seguimiento y evaluación. Estará a cargo de** La Junta de Inteligencia Conjunta realizar seguimiento y evaluación periódica al cumplimiento de los requerimientos de inteligencia y contrainteligencia establecidos en el Plan Nacional de Inteligencia.

g. **Vigencia.** El Plan Nacional de Inteligencia tendrá una vigencia de un (1) año a partir de su adopción.

CAPITULO III

Coordinación, cooperación y colaboración

Artículo 3. Coordinación y Cooperación para el intercambio de información. En el marco del cumplimiento de sus funciones los organismos de inteligencia y contrainteligencia deberán compartir información de acuerdo con la misión constitucional, legal y conforme a las competencias y principio de especialidad. Cada entidad será responsable de manejar la información que se comparta con la debida reserva y observando los protocolos de seguridad y acceso de la información establecidos por la Junta de Inteligencia Conjunta JIC.

Cuando se intercambie información con organismos o entidades homólogas de orden nacional o internacional, los Jefes o Directores de los organismos de inteligencia y contrainteligencia podrán suscribir los acuerdos, protocolos y/o memorandos de entendimiento, en los que se deben fijar con claridad los parámetros que garanticen la reserva legal, la seguridad de la información y las restricciones legales a la difusión de la misma.

Los acuerdos, protocolos y/o memorandos de entendimiento deberán estar ajustados a la Constitución, a la ley 1621 de 2013 y los decretos específicos en materia de la función y actividades de inteligencia y contrainteligencia.

Los Jefes y Directores de los organismos de inteligencia y contrainteligencia podrán suscribir directamente acuerdos, convenios y protocolos con los organismos homólogos, nacionales e internacionales, en los cuales se garantice la reserva legal, la seguridad y la protección de la información.

Tratándose de intercambio de información con organismos internacionales se establecerán y ajustarán los instrumentos internacionales, convenios, tratados y protocolos para establecer su uso, garantizar la reserva legal, la seguridad de la misma y evitar la difusión no autorizada a terceros.

Artículo 4. Colaboración de otras entidades públicas y privadas en el suministro de información. En el marco de la colaboración y coordinación interinstitucional, con el fin de requerir información útil y necesaria para la función de inteligencia y contrainteligencia del Estado, los Jefes o Directores de los organismos de inteligencia y contrainteligencia, podrán suscribir, convenios, acuerdos o protocolos interinstitucionales con otras entidades públicas y privadas, de acuerdo con lo consagrado en el artículo 42 de la ley 1621 de 2013.

CAPITULO IV

Documentos de inteligencia y contrainteligencia, órdenes de operaciones y/o misiones de trabajo

Artículo 5. Documentos de Inteligencia y Contrainteligencia. Son documentos de inteligencia y contrainteligencia todos aquellos originados, procesados y/o producidos en los organismos de inteligencia y contrainteligencia con los niveles de clasificación establecidos en el presente decreto. Estos documentos de conformidad con la ley están protegidos por la reserva legal.

Vo.Bo.: DIRECTOR ASUNTOS LEGALES
Vo.Bo. COORDINADORA GRUPO NEGOCIOS GENERALES
Revisó: Mtr. VÍCTOR HUGO PEÑA JIMÉNEZ

DECRETO NÚMERO 857 **DE 2014** **HOJA No. 4**

Continuación del Decreto. "Por el cual se reglamenta la Ley Estatutaria 1621 del 17 de abril de 2013, "Por medio de la cual se expiden normas para fortalecer el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, cumplir con su misión constitucional y legal, y se dictan otras disposiciones".

Los documentos de inteligencia y contrainteligencia pueden estar contenidos en medios físicos, digitales o similares, de acuerdo con los desarrollos científicos o tecnológicos y deben encontrarse bajo la administración, protección, custodia y seguridad de los organismos de inteligencia y contrainteligencia, los receptores autorizados o las entidades del Estado que de acuerdo con la ley deban conocer de ellos.

Artículo 6. Protección de los documentos de inteligencia y contrainteligencia. De conformidad con la ley, los documentos de inteligencia y contrainteligencia estarán amparados, en todo momento, por la reserva legal en cualquiera de los niveles de clasificación que se les asigne. La difusión contenida en estos documentos de inteligencia y contrainteligencia observará los parámetros y restricciones consagrados en la Constitución, la Ley 1621 de 2013, el presente decreto, los manuales y protocolos que se establezcan al interior de cada organismo para su adecuada administración, protección, custodia y seguridad de la información.

Artículo 7. Orden de Operaciones y/o Misión de Trabajo. Las órdenes de operaciones y/o misión de trabajo de inteligencia y contrainteligencia serán los documentos soportes básicos de las actividades de inteligencia y contrainteligencia y deberán contener:

a. Marco jurídico. Referencia de las normas legales en que se sustenta.

b. Motivación. Indicará el literal o literales correspondientes del artículo 4 de la ley 1621 de 2013 que sustenta o sustentan la actividad de inteligencia o contrainteligencia. Incluirá la relación entre la actividad de inteligencia, los fines y la ponderación respecto de los principios consagrados en el artículo 5 de la ley 1621 de 2013.

c. Planeamiento de la actividad: Contemplará las actividades, medios y recursos.

d. Dependencia o unidad que desarrollará la operación y/o actividad.

e. Personal que efectuará la misión.

f. Nivel de clasificación del documento.

g. Anexos cuando se consideren pertinentes.

h. Firma del jefe o director del organismo, o jefe o subjefe de unidad, sección o dependencia, según el equivalente en cada organismo, de conformidad con su estructura interna y atendiendo los criterios establecidos en el artículo 14 y 15 de la Ley 1621 de 2013. Los Jefes o Directores de los Organismos que integran la comunidad de inteligencia, deberán establecer por medio de acto administrativo los niveles de autorización para la emisión de órdenes de operaciones y/o misiones de trabajo.

i. Vigencia.

Parágrafo. Las órdenes de operaciones y/o misión de trabajo de inteligencia y contrainteligencia deberán observar los postulados consagrados en la Constitución, la Ley estatutaria propia de la función de inteligencia y contrainteligencia, la Ley de gastos reservados, los decretos reglamentarios que se expidan sobre la materia, la estrategia que en materia de inteligencia emita el Gobierno Nacional para su periodo constitucional, el Plan Nacional de Inteligencia, los requerimientos adicionales, los manuales y los demás actos administrativos correspondientes a inteligencia y contrainteligencia que expidan los respectivos organismos.

Artículo 8. Criterio orientador de los informes de inteligencia financiera de la U.I.A.F. Sin perjuicio de la información que obtenga de las unidades homologas de inteligencia financiera de otros países y de los reportes de operaciones sospechosas que por su naturaleza y de acuerdo con las prescripciones legales reciba la Unidad de Información y Análisis Financiero - UIAF, este organismo podrá con base en la información que reciba de los organismos que hacen parte de la comunidad de inteligencia del Estado, iniciar una misión de trabajo que de origen a informes de inteligencia financiera como criterio orientador con destino a las fiscalías competentes, de conformidad con el parágrafo del artículo 34 de la ley 1621 de 2013.

CAPITULO V

Manuales

Artículo 9. Manuales. Los Jefes o Directores de los organismos que integran la comunidad de inteligencia establecerán los contenidos, adoptarán y expedirán los manuales de inteligencia y contrainteligencia en cada uno de sus organismos, derogando aquellas disposiciones contrarias a la Constitución y a la ley 1621 de 2013.

Vo.Bo.: DIRECTOR ASUNTOS LEGALES
Vo.Bo. COORDINADORA GRUPO NEGOCIOS GENERALES
Revisó: MY. VÍCTOR HUGO PEÑA JIMÉNEZ

Anexo C. (continuación)

Los manuales deberán ser revisados y actualizados periódicamente, dejando constancia de la fecha en que se revisan o actualizan, de los cambios que se efectúan y de la fecha a partir de la cual entran en vigencia las modificaciones.

Los manuales y los demás documentos que hagan parte de ellos tendrán el nivel de clasificación que establezca cada organismo y mantendrán la reserva legal, de acuerdo con la Constitución, la ley estatutaria vigente en materia de inteligencia y contrainteligencia y el presente decreto reglamentario.

CAPITULO VI

Reserva legal, niveles de clasificación, sistema para la designación de los niveles de acceso a la información y desclasificación de documentos

Artículo 10. Reserva legal. En los términos del artículo 33 de la ley 1621 de 2013, los documentos, información y elementos técnicos de los organismos de inteligencia y contrainteligencia estarán amparados por la reserva legal y se les asignará un nivel de clasificación de acuerdo con lo establecido en el siguiente artículo.

Artículo 11. Niveles de clasificación de la información. Los niveles de clasificación de seguridad de la información que goza de reserva legal serán los siguientes:

a. **Ultrasecreto**. Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar al exterior del país los intereses del Estado o las relaciones internacionales.

b. **Secreto.** Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar al interior del país los intereses del Estado.

c. **Confidencial.** Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar directamente las instituciones democráticas.

d. **Restringido.** Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información de las instituciones militares, de la Policía Nacional o de los organismos y dependencias de inteligencia y contrainteligencia, sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar en las citadas instituciones y organismos, su seguridad, operaciones, medios, métodos, procedimientos, integrantes y fuentes.

Parágrafo. Los documentos de inteligencia y contrainteligencia que contengan información relacionada con diferentes niveles de clasificación de seguridad, asumirán la del nivel más alto que tenga la información contenida en ellos.

Sin perjuicio de lo establecido en el artículo 34 de la ley 1621 de 2013, a mayor nivel de clasificación de seguridad de la información, mayores serán las restricciones y controles para el acceso a la misma por parte de los receptores, las autoridades, los servidores públicos y asesores que deban conocer de ella. Estas restricciones deberán quedar establecidas en actos administrativos, manuales, protocolos, tarjetas de autorización para manejo y acceso a la información y contratos respectivos en cada uno de los organismos de inteligencia y contrainteligencia.

Artículo 12. Criterios para dar acceso a la información. Los organismos de inteligencia y contrainteligencia para dar acceso interno y externo a la información que goza de reserva legal y tenga nivel de clasificación, cumplirán con los siguientes criterios:

a. Mantener el principio de compartimentación a partir de la necesidad de saber y conocer estrictamente lo necesario para el desempeño de la función que le es propia. Así mismo, establecerán un mecanismo interno que determine los niveles de acceso para cada funcionario o asesor del organismo de inteligencia y contrainteligencia.

b. Entre mayor sea el nivel de clasificación de la información, mayores serán las restricciones como los controles que se deben aplicar para tener acceso a ella.

c. Identificar a los receptores de productos de inteligencia y contrainteligencia, estableciendo su nivel de acceso.

d. Desarrollar guías y/o protocolos, cuando sea el caso, para recibir, compartir e intercambiar información de inteligencia y contrainteligencia.

Vo.Bo.: DIRECTOR ASUNTOS LEGALES
Vo.Bo. COORDINADORA GRUPO NEGOCIOS GENERALES
Revisó: MY. VÍCTOR HUGO PEÑA JIMÉNEZ

Anexo C. (continuación)

e. Implementar de forma física y/o mediante la utilización de herramientas tecnológicas, el sistema de acceso a los diferentes niveles de clasificación, con capacidades de administración, monitoreo y control, con base en los cargos, perfiles y funciones determinadas en la estructura de cada organismo de inteligencia y contrainteligencia.

f. Suscribir acuerdos, protocolos o convenios, en los términos de la Constitución y la Ley, para recibir, compartir o intercambiar información que goce de reserva legal con agencias de inteligencia y contrainteligencia extranjeras.

Cada organismo documentará sus procedimientos, en sus manuales o protocolos, para asegurar la reserva legal, los niveles de clasificación y dar acceso a la información a las autoridades o receptores competentes.

CAPITULO VII

Seguridad y restricciones en la difusión de productos e información de inteligencia y contrainteligencia

Artículo 13. Seguridad y restricciones en la difusión de productos de inteligencia y contrainteligencia. Los organismos y dependencias de inteligencia y contrainteligencia deberán para los casos de difusión de productos de inteligencia y contrainteligencia a los receptores autorizados por la ley, indicar la reserva legal a la que está sometida la información y expresar, al receptor autorizado de la misma, si se trata de un producto de inteligencia o contrainteligencia "de solo conocimiento" o "de uso exclusivo", teniendo como referencia las siguientes restricciones para cada caso, así:

a. **De solo conocimiento.** Es aquel producto de inteligencia y contrainteligencia que tiene un receptor autorizado por ley, solo para conocimiento directo y, únicamente, como referencia o criterio orientador para tomar decisiones dentro de su órbita funcional. El receptor autorizado recibe el producto bajo las más estrictas medidas de seguridad, reserva legal y protocolos adecuados. El receptor autorizado no podrá difundir la información contenida en el producto de inteligencia y contrainteligencia.

b. **De uso exclusivo**. Es aquel producto de inteligencia y contrainteligencia que tiene un receptor autorizado por ley, solo para su conocimiento directo y uso exclusivo. Este producto sólo podrá ser empleado como referencia para tomar decisiones dentro de su órbita funcional. El receptor autorizado recibe el producto, bajo las más estrictas medidas de seguridad, reserva legal y protocolos adecuados. El receptor autorizado podrá difundir esta clase de información bajo su responsabilidad, únicamente, para establecer cursos de acción que permitan la toma de decisiones para el cumplimiento de los fines establecidos en la Constitución y la ley.

En ninguno de los anteriores casos, se podrá revelar fuentes, métodos, procedimientos, identidad de quienes desarrollan o desarrollaron actividades de inteligencia y contrainteligencia o poner en peligro la seguridad y defensa nacional.

Las autoridades competentes y los receptores de productos de inteligencia o contrainteligencia deberán garantizar, en todo momento, la reserva legal de la misma.

No se entregarán productos de inteligencia y contrainteligencia a aquellas autoridades competentes o receptores autorizados que no garanticen, por escrito, la reserva legal, la seguridad y la protección de la información contenida en los documentos o informes que les vayan a ser suministrados.

El documento con el cual se traslade la reserva legal de la información, a las autoridades competentes o receptores autorizados, deberá especificar la prohibición de emitir copias o duplicados de la misma, alertando sobre las acciones penales y disciplinarias que acarrea la no observancia de lo consagrado en la ley.

Artículo 14. Suministro de información. Cuando proceda, el organismo de inteligencia y contrainteligencia, responsable de dar respuesta legal a un requerimiento de información de inteligencia, deberá verificar previamente que:

a. La solicitud se ajuste a lo preceptuado en el artículo 34 de la Ley 1621 de 2013.

b. La respuesta identifique el nivel de clasificación, correspondiente a la naturaleza del documento o la información que se ponga en conocimiento de la autoridad competente.

c. La respuesta debe reflejar adecuadamente la valoración de la información, el uso de términos condicionales y dubitativos, que garantice entre otros la reserva, el debido proceso, el buen nombre y el derecho a la intimidad.

Vo.Bo.: DIRECTOR ASUNTOS LEGALES
Vo.Bo.: COORDINADORA GRUPO NEGOCIOS GENERALES
Revisó: MY. VÍCTOR HUGO PEÑA JIMÉNEZ

d. La respuesta cumpla los protocolos de seguridad, acceso y reserva.

e. La respuesta con la información suministrada no debe poner en peligro o riesgo la seguridad y defensa nacional, y, en los organismos que integran la comunidad de inteligencia, sus métodos, sus procedimientos, sus medios, sus fuentes, sus agentes, sus servidores públicos o sus asesores. Los criterios de valoración y ponderación del presente literal los fijará el Jefe o Director de cada organismo, según corresponda.

f. La respuesta no debe dar a conocer capacidades, procedimientos, métodos, medios, elementos técnicos, fuentes, operaciones o actividades de inteligencia o contrainteligencia.

g. La respuesta debe quedar debidamente registrada para tener la trazabilidad de la misma. En el documento de respuesta se debe trasladar a las autoridades competentes o receptores autorizados la reserva legal de la información y especificar las prohibiciones o restricciones de su difusión, alertando sobre las acciones penales y disciplinarias que acarrea la no observancia de lo consagrado en la ley.

CAPITULO VIII

Centros de Protección de Datos de Inteligencia y Contrainteligencia

Artículo 15. Centros de Protección de Datos de Inteligencia y Contrainteligencia (CPD). Los Jefes o Directores de cada uno de los organismos de inteligencia y contrainteligencia implementarán y/o adecuarán los CPD y archivos de inteligencia y contrainteligencia, designando un responsable por cada CPD en cada una de las dependencias, según su órbita funcional, nivel de clasificación de la información, desarrollo de la función en sus actividades estratégicas, operacionales o tácticas, o sus equivalentes, en cada uno de los organismos que hacen parte de la comunidad de inteligencia.

Los Jefes o Directores de inteligencia y contrainteligencia implementarán un plan anual de capacitación, para el personal responsable y comprometido en el ingreso, permanencia, difusión y protección de la información de inteligencia y contrainteligencia, en los CPD y en los archivos respectivos, que permita dar cumplimiento a los fines, límites y principios de la Ley 1621 de 2013.

Artículo 16. Actualización, corrección y retiro de datos y archivos de inteligencia. Para atender lo establecido en el artículo 31 de la Ley 1621 de 2013, los Jefes o Directores de los organismos de inteligencia y contrainteligencia crearán un comité para la actualización, corrección y retiro de datos y archivos de inteligencia.

El comité de actualización, corrección y retiro de datos y archivos de inteligencia en cada uno de los organismos que integran la comunidad de inteligencia, para efectos de fijar los criterios de actualización, corrección y retiro de datos y archivos de inteligencia y contrainteligencia, deberá observar los límites, fines y principios de los artículos 4 y 5 de la ley 1621 de 2013.

Una vez conformado el comité de actualización, corrección y retiro de datos y archivos de inteligencia en cada uno de los organismos que integran la comunidad de inteligencia, este comité deberá presentar al Jefe o Director del organismo de inteligencia y contrainteligencia, un primer informe de avance e implementación dentro de los seis meses siguientes a su conformación y, posteriormente, el comité presentará un informe periódico, cada cuatro meses, o, en forma extraordinaria, cuando lo requiera el Jefe o Director del organismo.

CAPITULO IX

Mecanismos de protección de la integridad e identidad de los servidores públicos de los organismos de inteligencia y contrainteligencia

Artículo 17. Protección de la identidad. Para garantizar la protección de la identidad de los servidores públicos que desarrollan actividades de inteligencia y contrainteligencia, la Registraduría Nacional del Estado Civil, en coordinación con las Direcciones y Jefaturas de Inteligencia de las Fuerzas Militares, la Policía Nacional, la Dirección Nacional de Inteligencia y la Unidad de Información y Análisis Financiero, establecerán mecanismos, manuales de procedimiento, formas de llevar los registros, trámites ágiles para la expedición del documento de nueva identidad, control de archivos y bases de datos, entre otros aspectos, que permitan mantener sistemas adecuados, seguros, confiables y reservados, a la hora de asignar nueva identidad con cupo numérico a quienes deban realizar misiones y operaciones de inteligencia y contrainteligencia previamente autorizadas.

El suministro de nueva identidad sólo se realizará previa solicitud escrita del respectivo Director o Jefe de Inteligencia y contrainteligencia, únicamente para las personas que él determine y que desarrollen misiones de trabajo en el marco de los artículos 4° y 5° de la Ley 1621 de 2013.

La nueva identidad sólo se suministrará por el tiempo necesario, prorrogable y controlable por quien autoriza, para cumplir con la misión y garantizar la protección e integridad del servidor público que en ella participe.

Vo.Bo.: DIRECTOR ASUNTOS LEGALES
Vo.Bo.: COORDINADORA GRUPO NEGOCIOS GENERALES
Revisó: MY. VÍCTOR HUGO PEÑA JIMÉNEZ

Los Comandantes de Fuerza, las Jefaturas y las Direcciones de los organismos de inteligencia y contrainteligencia adoptarán los procedimientos administrativos, académicos y demás que sean necesarios para facilitar la protección de la identidad funcional e instruir a los servidores públicos que harán uso de ella.

Parágrafo. El Director o Jefe de Inteligencia y contrainteligencia será quien determine el tiempo necesario y tendrá la potestad de requerir, en el momento que lo estime pertinente, la cancelación de la nueva identidad, mediante documento escrito clasificado dirigido al Registrador Nacional del Estado Civil.

Artículo 18. Medidas de seguridad. La Registraduría Nacional del Estado Civil, en coordinación con los organismos de inteligencia y contrainteligencia, establecerá los protocolos, medidas de seguridad y mecanismos necesarios, incluyendo estudios de seguridad y pruebas de confiabilidad de los funcionarios responsables de la administración del sistema de nueva identidad, garantizando en todo momento y lugar la reserva legal.

Artículo 19. Mecanismos de protección para los servidores públicos que desarrollan actividades de inteligencia y contrainteligencia y su núcleo familiar. Para garantizar la debida protección de los servidores públicos pertenecientes a los organismos que desarrollan actividades de inteligencia y contrainteligencia, que con ocasión del cumplimiento de sus funciones y actividades se vean compelidos a riesgo o amenaza, actual e inminente, contra su integridad personal o la de su núcleo familiar, las Direcciones y Jefaturas de Inteligencia de las Fuerzas Militares, la Policía Nacional, la Dirección Nacional de Inteligencia, la UIAF y de los demás organismos de inteligencia y contrainteligencia que se creen por ley, coordinarán la realización del estudio técnico de nivel de amenaza o riesgo, para la toma de las decisiones a que haya lugar, con la dependencia de contrainteligencia, su equivalente o se apoyarán con otro organismo de la comunidad de inteligencia para tal fin.

El estudio técnico de nivel de amenaza o riesgo, para la toma de decisiones en materia de protección, se realizará al servidor público perteneciente a un organismo de inteligencia y contrainteligencia que se encuentre por sus funciones en situación de amenaza o riesgo, y, cuando sea el caso, se efectuará al núcleo familiar de dicho servidor, siempre que estén dentro del primer grado de consanguinidad, primero de afinidad, primero civil, cónyuge, compañero o compañera permanente.

Los Comandantes de Fuerza, las Jefaturas y las Direcciones de los organismos de inteligencia y contrainteligencia adoptarán los procedimientos que sean necesarios para implementar los mecanismos de protección para los servidores públicos que desarrollan actividades de inteligencia y contrainteligencia y su núcleo familiar.

Los Comandantes de Fuerza, los Jefes y los Directores de los organismos de inteligencia y contrainteligencia adelantarán los trámites legales y las coordinaciones directas para garantizar las medidas de protección que se estimen necesarias y pertinentes.

Parágrafo 1: Las hojas de vida, los perfiles o los datos de los servidores públicos de inteligencia y contrainteligencia y de los contratistas que lleven a cabo estas actividades, no deberán ser revelados, incorporados, ni publicados en páginas y/o portales electrónicos o web u otros medios similares.

Parágrafo 2: Las autoridades competentes que por razón de sus funciones conozcan acerca de la identidad y actividades propias de los servidores públicos de los organismos de inteligencia y contrainteligencia, deberán garantizar la reserva legal de dicha información como mecanismo de protección.

CAPITULO X

Estudios de credibilidad y confiabilidad e ingreso y retiro de personal de los organismos de inteligencia y contrainteligencia.

Artículo 20. Estudios de credibilidad y confiabilidad. Los estudios de credibilidad y confiabilidad, son de obligatorio acatamiento y comprenden un conjunto de actividades, exámenes y/o evaluaciones, orientadas a asegurar los más altos estándares en materia de seguridad y reserva de la información, mediante la aplicación de exámenes técnicos o evaluaciones periódicas que verifiquen la idoneidad, credibilidad y confiabilidad de los servidores públicos y/o contratistas de los organismos de inteligencia y contrainteligencia y/o de personas que por razón de sus funciones y actividades tengan que conocer información con nivel de clasificación.

En este sentido, los estudios de credibilidad y confiabilidad podrán componerse, entre otros similares, de los siguientes exámenes técnicos que evalúen los siguientes aspectos:

a. **Individual:** Verificación administrativa de información y datos, referencias, anotaciones, antecedentes judiciales, antecedentes disciplinarios, antecedentes médicos, prueba y evaluación psicotécnica, entrevistas, competencias, prueba informatizada de integridad y veracidad, examen psicofisiológico de poligrafo.

b. **Familiar:** Visita domiciliaria y de vecindario.

c. **Social:** Estudio socioeconómico, referencias personales, profesionales, laborales, comerciales y financieras.

Vo.Bo.: DIRECTOR ASUNTOS LEGALES
Vo.Bo. COORDINADORA GRUPO NEGOCIOS GENERALES
Revisó: MY. VÍCTOR HUGO PEÑA JIMÉNEZ

Anexo C. (continuación)

DECRETO NÚMERO 857 **DE 2014** **HOJA No.** 9

Continuación del Decreto. "Por el cual se reglamenta la Ley Estatutaria 1621 del 17 de abril de 2013, "Por medio de la cual se expiden normas para fortalecer el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, cumplir con su misión constitucional y legal, y se dictan otras disposiciones".

Cada organismo de inteligencia y contrainteligencia determinará el objeto, finalidad y alcance de los estudios de credibilidad y confiabilidad, sus características, ámbito de aplicación, periodicidad, protocolos y procedimientos de realización y evaluación, privilegiando el interés general y la dignidad de los evaluados.

Los organismos de inteligencia y contrainteligencia podrán coordinar su realización con otras dependencias y extenderlos a los procesos y procedimientos internos en cada institución, siempre que tengan relación directa con las actividades de inteligencia, contrainteligencia y los demás fines enunciados en la ley 1621 de 2013.

Parágrafo 1. Los organismos que integran la comunidad de inteligencia, cuando las circunstancias lo requieran, podrán apoyarse entre sí o con organismos homólogos internacionales, para la coordinación y realización de estudios de credibilidad y confiabilidad, con el fin de optimizar las fortalezas institucionales en materia de conocimiento específico, recursos humanos y recursos técnicos especializados.

Para la aplicación de las pruebas de credibilidad y confianza, el nivel de acceso a la información que se haya dado al funcionario y el nivel que posea para la autorización de cada operación o misión de trabajo, cuando fuere el caso, serán factores decisivos para el diseño e implementación del conjunto de exámenes a practicar al funcionario.

Parágrafo 2. Los organismos de inteligencia y contrainteligencia desarrollarán protocolos internos para la aplicación de las pruebas de credibilidad y confiabilidad, cuando se trate de actividades específicas, de apoyo dirigido a la recolección de información a través de fuentes humanas y, de la dirección, orientación y coordinación de equipos especializados de inteligencia, contrainteligencia o asuntos internos, entre otros.

CAPITULO XI

Otras disposiciones

Artículo 21. Programas de formación y capacitación del personal de inteligencia y contrainteligencia. Los organismos de inteligencia y contrainteligencia, en el marco de su naturaleza jurídica crearán, orientarán y/o implementarán programas académicos para formar, instruir, capacitar periódicamente a los servidores públicos que cumplan funciones relacionadas con las actividades de inteligencia y contrainteligencia, y expedirán los certificados de idoneidad y las constancias sobre el desarrollo y aprobación de dichos programas.

Parágrafo. Para asegurar la formación, instrucción, capacitación y adiestramiento de los servidores públicos, los organismos que integran la comunidad de inteligencia podrán apoyarse entre sí o con otras entidades del orden nacional o internacional.

Artículo 22. Los organismos de inteligencia y contrainteligencia que conforman la comunidad de inteligencia tramitarán la partida presupuestal – Gastos Generales – Gastos Reservados con cargo a su asignación presupuestal, observando el conducto regular, a fin de atender las diferentes actividades de inteligencia y contrainteligencia asignadas de conformidad con su marco legal.

Artículo 23. Vigencia y derogatoria. El presente decreto rige a partir de la fecha de su publicación, y deroga las normas que le sean contrarias.

PUBLÍQUESE Y CÚMPLASE
Dado en Bogotá D.C., 2 MAY 2014

EL MINISTRO DE HACIENDA Y CRÉDITO PÚBLICO,

MAURICIO CÁRDENAS SANTAMARÍA

Vo.Bo.: DIRECTOR ASUNTOS LEGALES
Vo.Bo.: COORDINADORA GRUPO NEGOCIOS GENERALES
Revisó: MY. VÍCTOR HUGO PEÑA JIMÉNEZ

Anexo C. (continuación)

DECRETO NÚMERO 857 **DE 2014** **HOJA No.** 10

Continuación del Decreto. "Por el cual se reglamenta la Ley Estatutaria 1621 del 17 de abril de 2013, "Por medio de la cual se expiden normas para fortalecer el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, cumplir con su misión constitucional y legal, y se dictan otras disposiciones".

EL MINISTRO DE DEFENSA NACIONAL,

JUAN CARLOS PINZÓN BUENO

EL DIRECTOR DEL DEPARTAMENTO ADMINISTRATIVO "DIRECCIÓN NACIONAL DE INTELIGENCIA".

Almirante (r) ÁLVARO ECHANDIA DURAN

LA DIRECTORA DEL DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA,

ELIZABETH RODRÍGUEZ TAYLOR

Anexo D. Ley 1712 de 2014

LEY No. 1712 6 MAR 2014

"POR MEDIO DE LA CUAL SE CREA LA LEY DE TRANSPARENCIA Y DEL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA NACIONAL Y SE DICTAN OTRAS DISPOSICIONES".

El Congreso de la República
DECRETA:

TÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Objeto. El objeto de la presente ley es regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.

Artículo 2. Principio de máxima publicidad para titular universal. Toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no podrá ser reservada o limitada sino por disposición constitucional o legal, de conformidad con la presente ley.

Artículo 3. Otros principios de la transparencia y acceso a la información pública. En la interpretación del derecho de acceso a la información se deberá adoptar un criterio de razonabilidad y proporcionalidad, así como aplicar los siguientes principios:

Principio de transparencia. Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta ley se presume pública, en consecuencia de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta ley.

Principio de buena fe. En virtud del cual todo sujeto obligado, al cumplir con las obligaciones derivadas del derecho de acceso a la información pública, lo hará con motivación honesta, leal y desprovista de cualquier intención dolosa o culposa.

Principio de facilitación. En virtud de este principio los sujetos obligados deberán facilitar el ejercicio del derecho de acceso a la información pública, excluyendo exigencias o requisitos que puedan obstruirlo o impedirlo.

Principio de no discriminación. De acuerdo al cual los sujetos obligados deberán entregar información a todas las personas que lo soliciten, en igualdad de condiciones, sin hacer distinciones arbitrarias y sin exigir expresión de causa o motivación para la solicitud.

1712

Principio de gratuidad. Según este principio el acceso a la información pública es gratuito y no se podrá cobrar valores adicionales al costo de reproducción de la información.

Principio de celeridad. Con este principio se busca la agilidad en el trámite y la gestión administrativa. Comporta la indispensable agilidad en el cumplimiento de las tareas a cargo de entidades y servidores públicos.

Principio de eficacia. El principio impone el logro de resultados mínimos en relación con las responsabilidades confiadas a los organismos estatales, con miras a la efectividad de los derechos colectivos e individuales.

Principio de la calidad de la información. Toda la información de interés público que sea producida, gestionada y difundida por el sujeto obligado, deberá ser oportuna, objetiva, veraz, completa, reutilizable, procesable y estar disponible en formatos accesibles para los solicitantes e interesados en ella, teniendo en cuenta los procedimientos de gestión documental de la respectiva entidad.

Principio de la divulgación proactiva de la información. El derecho de acceso a la información no radica únicamente en la obligación de dar respuesta a las peticiones de la sociedad, sino también en el deber de los sujetos obligados de promover y generar una cultura de transparencia, lo que conlleva la obligación de publicar y divulgar documentos y archivos que plasman la actividad estatal y de interés público, de forma rutinaria y proactiva, actualizada, accesible y comprensible, atendiendo a límites razonables del talento humano y recursos físicos y financieros.

Principio de responsabilidad en el uso de la información. En virtud de este, cualquier persona que haga uso de la información que proporcionen los sujetos obligados, lo hará atendiendo a la misma.

Artículo 4. Concepto del derecho. En ejercicio del derecho fundamental de acceso a la información, toda persona puede conocer sobre la existencia y acceder a la información pública en posesión o bajo control de los sujetos obligados. El acceso a la información solamente podrá ser restringido excepcionalmente. Las excepciones serán limitadas y proporcionales, deberán estar contempladas en la ley o en la Constitución y ser acordes con los principios de una sociedad democrática.

El derecho de acceso a la información genera la obligación correlativa de divulgar proactivamente la información pública y responder de buena fe, de manera adecuada, veraz, oportuna y accesible a las solicitudes de acceso, lo que a su vez conlleva la obligación de producir o capturar la información pública. Para cumplir lo anterior los sujetos obligados deberán implementar procedimientos archivísticos que garanticen la disponibilidad en el tiempo de documentos electrónicos auténticos.

Parágrafo. Cuando el usuario considere que la solicitud de la información pone en riesgo su integridad o la de su familia, podrá solicitar ante el Ministerio Público el procedimiento especial de solicitud con identificación reservada.

Artículo 5. Ámbito de aplicación. Las disposiciones de esta ley serán aplicables a las siguientes personas en calidad de sujetos obligados:

2

a) Toda entidad pública, incluyendo las pertenecientes a todas las Ramas del Poder Público, en todos los niveles de la estructura estatal, central o descentralizada por servicios o territorialmente, en los órdenes nacional, departamental, municipal y distrital;

b) Los órganos, organismos y entidades estatales independientes o autónomos y de control;

c) Las personas naturales y jurídicas, públicas o privadas, que presten función pública, que presten servicios públicos respecto de la información directamente relacionada con la prestación del servicio público;

d) Cualquier persona natural, jurídica o dependencia de persona jurídica que desempeñe función pública o de autoridad pública, respecto de la información directamente relacionada con el desempeño de su función;

e) Los partidos o movimientos políticos y los grupos significativos de ciudadanos;

f) Las entidades que administren instituciones parafiscales, fondos o recursos de naturaleza u origen público.

Las personas naturales o jurídicas que reciban o intermedien fondos o beneficios públicos territoriales y nacionales y no cumplan ninguno de los otros requisitos para ser considerados sujetos obligados, sólo deberán cumplir con la presente ley respecto de aquella información que se produzca en relación con fondos públicos que reciban o intermedien.

Parágrafo 1. No serán sujetos obligados aquellas personas naturales o jurídicas de carácter privado que sean usuarios de información pública.

Artículo 6. Definiciones.

a) **Información.** Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

b) **Información pública.** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

c) **Información pública clasificada.** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semi-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley.

d) **Información pública reservada.** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley.

e) **Publicar o divulgar**. Significa poner a disposición en una forma de acceso general a los miembros del público e incluye la impresión, emisión y las formas electrónicas de difusión.

f) **Sujetos obligados.** Se refiere a cualquier persona natural o jurídica, pública o privada incluida en el artículo 5° de esta ley.

g) **Gestión documental.** Es el conjunto de actividades administrativas y técnicas tendientes a la planificación, procesamiento, manejo y organización de la documentación producida y recibida por los sujetos obligados, desde su origen hasta su destino final, con el objeto de facilitar su utilización y conservación.

h) **Documento de archivo.** Es el registro de información producida o recibida por una entidad pública o privada en razón de sus actividades o funciones.

i) **Archivo**. Es el conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura.

j) **Datos Abiertos**. Son todos aquello datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitar su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

k) **Documento en construcción.** No será considerada información pública aquella información preliminar y no definitiva, propia del proceso deliberatorio de un sujeto obligado en su calidad de tal.

TÍTULO II
DE LA PUBLICIDAD Y DEL CONTENIDO DE LA INFORMACIÓN

Artículo 7. Disponibilidad de la Información. En virtud de los principios señalados, deberá estar a disposición del público la información a la que hace referencia la presente ley, a través de medios físicos, remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas dicha información en la Web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten.

Anexo D. (continuación)

1712

Parágrafo. Se permite en todo caso la retransmisión de televisión por internet cuando el contenido sea información pública de entidades del estado o noticias al respecto.

Artículo 8. Criterio diferencial de accesibilidad. Con el objeto de facilitar que las poblaciones específicas accedan a la información que particularmente las afecte, los sujetos obligados, a solicitud de las autoridades de las comunidades, divulgarán la información pública en diversos idiomas y lenguas y elaborarán formatos alternativos comprensibles para dichos grupos. Deberá asegurarse el acceso a esa información a los distintos grupos étnicos y culturales del país y en especial se adecuarán los medios de comunicación para que faciliten el acceso a las personas que se encuentran en situación de discapacidad.

Artículo 9. Información mínima obligatoria respecto a la estructura del sujeto obligado. Todo sujeto obligado deberá publicar la siguiente información mínima obligatoria de manera proactiva en los sistemas de información del Estado o herramientas que lo sustituyan:

a) La descripción de su estructura orgánica, funciones y deberes, la ubicación de sus sedes y áreas, divisiones o departamentos, y sus horas de atención al público;

b) Su presupuesto general, ejecución presupuestal histórica anual y planes de gasto público para cada año fiscal, de conformidad con el artículo 74 de la ley 1474 de 2011;

c) Un directorio que incluya el, cargo, direcciones de correo electrónico y teléfono del despacho de los empleados y funcionarios y las escalas salariales correspondientes a las categorías de todos los servidores que trabajan en el sujeto obligado, de conformidad con el formato de información de servidores públicos y contratistas;

d) Todas las normas generales y reglamentarias, políticas, lineamientos o manuales, las metas y objetivos de las unidades administrativas de conformidad con sus programas operativos y los resultados de las auditorías al ejercicio presupuestal e indicadores de desempeño;

e) Su respectivo plan de compras anual, así como las contrataciones adjudicadas para la correspondiente vigencia en lo relacionado con funcionamiento e inversión, las obras públicas, los bienes adquiridos, arrendados y en caso de los servicios de estudios o investigaciones deberá señalarse el tema específico, de conformidad con el artículo 74 de la ley 1474 de 2011. En el caso de las personas naturales con contratos de prestación de servicios, deberá publicarse el objeto del contrato, monto de los honorarios y direcciones de correo electrónico, de conformidad con el formato de información de servidores públicos y contratistas;

f) Los plazos de cumplimiento de los contratos;

g) Publicar el Plan Anticorrupción y de Atención al Ciudadano, de conformidad con el artículo 73 de la ley 1474 de 2011.

5

Anexo D. (continuación)

Parágrafo 1º. La información a que se refiere este artículo deberá publicarse de tal forma que facilite su uso y comprensión por las personas, y que permita asegurar su calidad, veracidad, oportunidad y confiabilidad.

Parágrafo 2º. En relación a los literales c) y e) del presente artículo, el Departamento Administrativo de la Función Pública establecerá un formato de información de los servidores públicos y de personas naturales con contratos de prestación de servicios, el cual contendrá los nombres y apellidos completos, ciudad de nacimiento, formación académica, experiencia laboral y profesional de los funcionarios y de los contratistas. Se omitirá cualquier información que afecte la privacidad y el buen nombre de los servidores públicos y contratistas, en los términos definidos por la constitución y la ley.

Parágrafo 3°: Sin perjuicio a lo establecido en el presente artículo los sujetos obligados deberán observar lo establecido por la estrategia de gobierno en línea, o a que haga sus veces, en cuanto a la publicación y divulgación de la información.

Artículo 10. Publicidad de la contratación. En el caso de la información de contratos indicada en el artículo 9 literal e), tratándose de contrataciones sometidas al régimen de contratación estatal, cada entidad publicará en el medio electrónico institucional sus contrataciones en curso y un vínculo al sistema electrónico para la contratación pública o el que haga sus veces, a través del cual podrá accederse directamente a la información correspondiente al respectivo proceso contractual, en aquellos que se encuentren sometidas a dicho sistema, sin excepción.

Parágrafo. Los sujetos obligados deberán actualizar la información a la que se refiere el artículo 9°, mínimo cada mes.

Artículo 11. Información mínima obligatoria respecto a servicios, procedimientos y funcionamiento del sujeto obligado. Todo sujeto obligado deberá publicar la siguiente información mínima obligatoria de manera proactiva:

a) Detalles pertinentes sobre todo servicio que brinde directamente al público, incluyendo normas, formularios y protocolos de atención;

b) Toda la información correspondiente a los trámites que se pueden agotar en la entidad, incluyendo la normativa relacionada, el proceso, los costos asociados y los distintos formatos o formularios requeridos;

c) Una descripción de los procedimientos que se siguen para tomar decisiones en las diferentes áreas;

d) El contenido de toda decisión y/o política que haya adoptado y afecte al público, junto con sus fundamentos y toda interpretación autorizada de ellas;

e) Todos los informes de gestión, evaluación y auditoría del sujeto obligado;

f) Todo mecanismo interno y externo de supervisión, notificación y vigilancia pertinente del sujeto obligado;

1712

g) Sus procedimientos, lineamientos, políticas en materia de adquisiciones y compras, así como todos los datos de adjudicación y ejecución de contratos, incluidos concursos y licitaciones;

h) Todo mecanismo de presentación directa de solicitudes, quejas y reclamos a disposición del público en relación con acciones u omisiones del sujeto obligado. Junto con un informe de todas las solicitudes, denuncias y los tiempos de respuesta del sujeto obligado;

i) Todo mecanismo o procedimiento por medio del cual el público pueda participar en la formulación de la política o el ejercicio de las facultades de ese sujeto obligado;

j) Un registro de publicaciones que contenga los documentos publicados de conformidad con la presente ley y automáticamente disponibles, así como un Registro de Activos de Información;

k) Los sujetos obligados deberán publicar datos abiertos, para lo cual deberán contemplar las excepciones establecidas en el título 3 de la presente ley. Adicionalmente, para las condiciones técnicas de su publicación, se deberán observar los requisitos que establezca el gobierno nacional a través del Ministerio de las Tecnologías de la Información y las Comunicaciones o quien haga sus veces.

Artículo 12. Adopción de esquemas de publicación. Todo sujeto obligado deberá adoptar y difundir de manera amplia su esquema de publicación, dentro de los seis meses siguientes a la entrada en vigencia de la presente ley. El esquema será difundido a través de su sitio Web, y en su defecto, en los dispositivos de divulgación existentes en su dependencia, incluyendo boletines, gacetas y carteleras. El esquema de publicación deberá establecer:

a) Las clases de información que el sujeto obligado publicará de manera proactiva y que en todo caso deberá comprender la información mínima obligatoria;

b) La manera en la cual publicará dicha información;

c) Otras recomendaciones adicionales que establezca el Ministerio Público,

d) Los cuadros de clasificación documental que faciliten la consulta de los documentos públicos que se conservan en los archivos del respectivo sujeto obligado, de acuerdo con la reglamentación establecida por el Archivo General de la Nación,

e) La periodicidad de la divulgación, acorde a los principios administrativos de la función pública.

Todo sujeto obligado deberá publicar información de conformidad con su esquema de publicación.

Artículo 13. Registros de Activos de Información. Todo sujeto obligado deberá crear y mantener actualizado el Registro de Activos de Información haciendo un listado de:

1712

a) Todas las categorías de información publicada por el sujeto obligado.

b) Todo registro publicado.

c) Todo registro disponible para ser solicitado por el público.

El Ministerio Público podrá establecer estándares en relación a los Registros Activos de Información.

Todo sujeto obligado deberá asegurarse de que sus Registros de Activos de Información cumplan con los estándares establecidos por el Ministerio Público y con aquellos dictados por el Archivo General de la Nación, en relación a la constitución de las Tablas de Retención Documental –TRD- y los inventarios documentales.

Artículo 14. Información publicada con anterioridad. Los sujetos obligados deben garantizar y facilitar a los solicitantes, de la manera más sencilla posible, el acceso a toda la información previamente divulgada. Se publicará esta información en los términos establecidos.

Cuando se dé respuesta a una de las solicitudes aquí previstas, esta deberá hacerse pública de manera proactiva en el sitio Web del sujeto obligado, y en defecto de la existencia de un sitio Web, en los dispositivos de divulgación existentes en su dependencia.

Artículo 15. Programa de Gestión Documental. Dentro de los seis (6) meses siguientes a la entrada en vigencia de la presente ley, los sujetos obligados deberán adoptar un Programa de Gestión Documental en el cual se establezcan los procedimientos y lineamientos necesarios para la producción, distribución, organización, consulta y conservación de los documentos públicos. Este Programa deberá integrarse con las funciones administrativas del sujeto obligado. Deberán observarse los lineamientos y recomendaciones que el Archivo General de la Nación y demás entidades competentes expidan en la materia.

Artículo 16. Archivos. En su carácter de centros de información institucional que contribuyen tanto a la eficacia y eficiencia del Estado en el servicio a ciudadano, como a la promoción activa del acceso a la información pública, los sujetos obligados deben asegurarse de que existan dentro de sus entidades procedimientos claros para la creación, gestión, organización y conservación de sus archivos. Los procedimientos adoptados deberán observar los lineamientos que en la materia sean producidos por el Archivo General de la Nación.

Artículo 17. Sistemas de información. Para asegurar que los sistemas de información electrónica sean efectivamente una herramienta para promover el acceso a la información pública, los sujetos obligados deben asegurar que estos:

a) Se encuentren alineados con los distintos procedimientos y articulados con los lineamientos establecidos en el Programa de Gestión Documental de la entidad;

b) Gestionen la misma información que se encuentre en los sistemas administrativos del sujeto obligado;

8

Anexo D. (continuación)

c) En el caso de la información de interés público, deberá existir una ventanilla en la cual se pueda acceder a la información en formatos y lenguajes comprensibles para los ciudadanos,

d) Se encuentren alineados con la estrategia de gobierno en línea o de la que haga sus veces.

TÍTULO III
EXCEPCIONES ACCESO A LA INFORMACIÓN

Artículo 18. Información exceptuada por daño de derechos a personas naturales o jurídicas. Es toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito, siempre que el acceso pudiere causar un daño a los siguientes derechos:

a) El derecho de toda persona a la intimidad, bajo las limitaciones propias que impone la condición de servidor público, en concordancia con lo estipulado.

b) El derecho de toda persona a la vida, la salud o la seguridad;

c) Los secretos comerciales, industriales y profesionales, así como los estipulados en el parágrafo del artículo 77 de la ley 1474 de 2011.

Parágrafo. Estas excepciones tene una duración ilimitada y no deberán aplicarse cuando la persona natural o jurídica ha consentido en la revelación de sus datos personales o privados o bien cuando es claro que la información fue entregada como parte de aquella información que debe estar bajo el régimen de publicidad aplicable.

Artículo 19. Información exceptuada por daño a los intereses públicos. Es toda aquella información pública reservada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito en las siguientes circunstancias, siempre que dicho acceso estuviere expresamente prohibido por una norma legal o constitucional:

a) La defensa y seguridad nacional.
b) La seguridad pública.
c) Las relaciones internacionales.
d) La prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso.
e) El debido proceso y la igualdad de las partes en los procesos judiciales.
f) La administración efectiva de la justicia.
g) Los derechos de la infancia y la adolescencia.
h) La estabilidad macroeconómica y financiera del país.
i) La salud pública.

Parágrafo. Se exceptúan también los documentos que contengan las opiniones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos.

Artículo 20. Índice de Información clasificada y reservada. Los sujetos obligados deberán mantener un índice actualizado de los actos, documentos e

Informaciones calificados como clasificados o reservados, de conformidad a esta ley. El índice incluirá sus denominaciones, la motivación y la individualización del acto en que conste tal calificación.

Artículo 21. Divulgación parcial y otras reglas. En aquellas circunstancias en que la totalidad de la información contenida en un documento no esté protegida por una excepción contenida en la presente ley, debe hacerse una versión pública que mantenga la reserva únicamente de la parte indispensable. La información pública que no cae en ningún supuesto de excepción deberá ser entregada a la parte solicitante, así como ser de conocimiento público. La reserva de acceso a la información opera respecto del contenido de un documento público pero no de su existencia.

Ninguna autoridad pública puede negarse a indicar si un documento obra o no en su poder o negar la divulgación de un documento.

las excepciones de acceso a la información contenidas en la presente ley no aplican en casos de violación de derechos humanos o delitos de lesa humanidad, y en todo caso deberán protegerse los derechos de las víctimas de dichas violaciones.

Artículo 22. Excepciones temporales. La reserva de las informaciones amparadas por el artículo 19, no deberá extenderse por un período mayor a quince (15) años.

TÍTULO IV
DE LAS GARANTÍAS AL EJERCICIO DEL DERECHO DE ACCESO A LA INFORMACIÓN

Artículo 23. Funciones del Ministerio Público. El Ministerio Público será el encargado de velar por el adecuado cumplimiento de las obligaciones estipuladas en la presente ley. Para tal propósito, la Procuraduría General de la Nación en un plazo no mayor a seis meses establecerá una metodología para que aquel cumpla las siguientes funciones y atribuciones:

a) Desarrollar acciones preventivas para el cumplimiento de esta ley.

b) Realizar informes sobre el cumplimiento de las decisiones de tutelas sobre acceso a la información.

c) Publicar las decisiones de tutela y normatividad sobre acceso a la información pública.

d) Promover el conocimiento y aplicación de la presente ley y sus disposiciones entre los sujetos obligados, así como su comprensión entre el público, teniendo en cuenta criterios diferenciales para su accesibilidad, sobre las materias de su competencia mediante la publicación y difusión de una guía sobre el derecho de acceso a la información.

e) Aplicar las sanciones disciplinarias que la presente ley consagra.

f) Decidir disciplinariamente, en los casos de ejercicio de poder preferente, los casos de faltas o mala conducta derivada del derecho de acceso a la información.

Anexo D. (continuación)

1712

g) Promover la transparencia de la función pública, el acceso y la publicidad de la información de las entidades del Estado, por cualquier medio de publicación.

h) Requerir a los sujetos obligados para que ajusten sus procedimientos y sistema de atención al ciudadano a dicha legislación.

i) Realizar, directamente o a través de terceros, actividades de capacitación de funcionarios públicos en materia de transparencia y acceso a la información.

j) Efectuar estadísticas y reportes sobre transparencia y acceso a la información de los órganos de la administración del Estado y sobre el cumplimiento de esta ley.

k) Entregar en debida forma las respuestas a las peticiones formuladas con solicitud de identificación reservada a las que se refiere el parágrafo del artículo 4º de la presente ley.

l) Implementar y administrar los sistemas de información en el cumplimiento de sus funciones para lo cual establecerá los plazos y criterios del reporte por parte de las entidades públicas que considere necesarias.

Las entidades del Ministerio Público contarán con una oficina designada que dispondrá de los medios necesarios para el cumplimiento de las anteriores funciones y atribuciones.

Artículo 24. Del Derecho de Acceso a la Información. Toda persona tiene derecho a solicitar y recibir información de cualquier sujeto obligado, en la forma y condiciones que establece esta ley y la Constitución.

Artículo 25. Solicitud de acceso a la Información Pública. Es aquella que, de forma oral o escrita, incluida la vía electrónica, puede hacer cualquier persona para acceder a la información pública.

Parágrafo. En ningún caso podrán ser rechazadas la petición por motivos de fundamentación inadecuada o incompleta.

Artículo 26. Respuesta a solicitud de acceso a información. Es aquel acto escrito mediante el cual, de forma oportuna, veraz, completa, motivada y actualizada, todo sujeto obligado responde materialmente a cualquier persona que presente una solicitud de acceso a información pública. Su respuesta se dará en los términos establecidos.

La respuesta a la solicitud deberá ser gratuita o sujeta a un costo que no supere el valor de la reproducción y envío de la misma al solicitante. Se preferirá, cuando sea posible, según los sujetos pasivo y activo, la respuesta por vía electrónica, con el consentimiento del solicitante.

Artículo 27. Recursos del solicitante. Cuando la respuesta a la solicitud de información invoque la reserva de seguridad y defensa nacional o relaciones internacionales, el solicitante podrá acudir al recurso de reposición, el cual deberá interponerse por escrito y sustentando en la diligencia de notificación, o dentro de los tres (3) días siguientes a ella.

Negado este recurso corresponderá al Tribunal administrativo con jurisdicción en el lugar donde se encuentren los documentos, si se trata de autoridades nacionales, departamentales o del Distrito Capital de Bogotá, o al juez administrativo si se trata de autoridades distritales y municipales, decidir en única instancia si se niega o se acepta, total o parcialmente, la petición formulada.

Para ello, el funcionario respectivo enviará la documentación correspondiente al tribunal o al juez administrativo en un plazo no superior a tres (3) días. En caso de que el funcionario incumpla esta obligación el solicitante podrá hacer el respectivo envío de manera directa.

El juez administrativo decidirá dentro de los diez (10) días siguientes. Este término se interrumpirá en los siguientes casos:

1. Cuando el tribunal o el juez administrativo solicite copia o fotocopia de los documentos sobre cuya divulgación deba decidir, o cualquier otra información que requieran, y hasta la fecha en la cual las reciba oficialmente.

2. Cuando la autoridad solicite, a la sección del Consejo de Estado que el reglamento disponga, asumir conocimiento del asunto en atención a su importancia jurídica o con el objeto de unificar criterios sobre el tema. Si al cabo de cinco (5) días la sección guarda silencio, o decide no avocar conocimiento, la actuación continuará ante el respectivo tribunal o juzgado administrativo.

Parágrafo. Será procedente la acción de tutela para aquellos casos no contemplados en el presente artículo, una vez agotado el recurso de reposición del Código Contencioso Administrativo.

Artículo 28. Carga de la prueba. Le corresponde al sujeto obligado aportar las razones y pruebas que fundamenten y evidencien que la información solicitada debe permanecer reservada o confidencial. En particular, el sujeto obligado debe demostrar que la información debe relacionarse con un objetivo legítimo establecido legal o constitucionalmente. Además, deberá establecer si se trata de una excepción contenida en los artículos 18 y 19 de esta ley y si la revelación de la información causaría un daño presente, probable y específico que excede el interés público que representa el acceso a la información.

Artículo 29. Responsabilidad Penal. Todo acto de ocultamiento, destrucción o alteración deliberada total o parcial de información pública, una vez haya sido objeto de una solicitud de información, será sancionada en los términos del artículo 292 del Código Penal.

TÍTULO V
VIGENCIA Y MEDIDAS DE PROMOCIÓN

Artículo 30. Capacitación. El Ministerio Público, con el apoyo de la sociedad civil interesada en participar, deberá asistir a los sujetos obligados y a la ciudadanía en la capacitación con enfoque diferencial, para la aplicación de esta ley.

Artículo 31. Educación Formal. El Ministerio de Educación, con el apoyo de la sociedad civil, deberá promover que en el área relacionada con el estudio de la Constitución, la instrucción cívica y el fomento de prácticas democráticas

Anexo D. (continuación)

1712

obligatorias para las instituciones educativas privadas y públicas, de conformidad con el artículo 41 de la Constitución Política, se incluya información sobre el derecho de acceso a la información, sus principios y sus reglas básicas.

Artículo 32. Política Pública de acceso a la información. El diseño, promoción e implementación de la política pública de acceso a la información pública, estará a cargo de la Secretaría de Transparencia de la Presidencia de la República, el Ministerio de Tecnología de la Información y Comunicaciones, el Departamento Administrativo de la Función Pública (DAFP), el Departamento Nacional de Planeación (DNP), el Archivo General de la Nación y el Departamento Administrativo Nacional de Estadística (DANE).

Artículo 33. Vigencia y derogatoria. La presente ley rige a los seis (6) meses de la fecha de su promulgación para todos los sujetos obligados del orden nacional. Para los entes territoriales la ley entrará en vigencia un año después de su promulgación. La presente ley deroga todas las disposiciones que le sean contrarias.

EL PRESIDENTE DEL H. SENADO DE LA REPUBLICA

JUAN FERNANDO CRISTO BUSTOS

EL SECRETARIO GENERAL DEL H. SENADO DE LA REPUBLICA

GREGORIO ELJACH PACHECO

EL PRESIDENTE DE LA H. CÁMARA DE REPRESENTANTES

HERNÁN PENAGOS GIRALDO

EL SECRETARIO GENERAL DE LA H. CÁMARA DE REPRESENTANTES

JORGE HUMBERTO MANTILLA SERRANO

Anexo D. (continuación)

LEY No. 1712 6 MAR 2014

"POR MEDIO DE LA CUAL SE CREA LA LEY DE TRANSPARENCIA Y DEL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA NACIONAL Y SE DICTAN OTRAS DISPOSICIONES"

REPÚBLICA DE COLOMBIA - GOBIERNO NACIONAL

PUBLÍQUESE Y CÚMPLASE

En cumplimiento de lo dispuesto en la Sentencia C-274 del 9 de mayo de 2013, proferida por la Corte Constitucional, se procede a la sanción del proyecto de Ley, toda vez que dicha Corporación ordena la remisión del expediente al Congreso de la República, para continuar el trámite legislativo de rigor y su posterior envío al Presidente de la República para efecto de la correspondiente sanción.

Dada en Bogotá, D.C., a los 6 MAR 2014

EL MINISTRO DE INTERIOR,

AURELIO IRAGORRI VALENCIA

EL MINISTRO DE JUSTICIA Y DEL DERECHO,

ALFONSO GÓMEZ MENDEZ

LA MINISTRA DE EDUCACIÓN NACIONAL,

MARÍA FERNANDA CAMPO SAAVEDRA

EL MINISTRO DE TECNOLOGÍAS, DE LA INFORMACIÓN Y LAS COMUNICACIONES,

DIEGO MOLANO VEGA

Anexo E. Informe entrevista GAHD

RESERVADO

MEMBRETE UNIDAD (Militar y/o Policía)

INFORME DE ENTREVISTA

Fotografía

UNIDAD .. :
LUGAR . :
FECHA :
No. Entrevista :

Articulo 453 del Código Penal Fraude Procesal: El que por cualquier medio fraudulento induzca en error a un servidor público para obtener sentencia, resolución o acto administrativo contrario a la ley, incurrirá en prisión de cuatro (4) a ocho (8) años multa de doscientos (200) a mil (1.000) salarios mínimos legales mensuales vigentes e inhabilitación para el ejercicio de derechos y funciones públicas de cinco (5) a ocho (8) años.

LA FINALIDAD DE ESTA ENTREVISTA ES EXCLUSIVAMENTE PARA CONSTATAR LA PERTENENCIA AL GRUPO ARMADO ILEGAL Y LA VOLUNTAD DE REINCORPORARSE A LA VIDA CIVIL. NO CONSTITUYE MEDIO DE PRUEBA PARA FINES JUDICIALES.

1.- DATOS GENERALES DEL ENTREVISTADO

Nombres y Apellidos

Alias o apodo

Organización a la que manifiesta haber pertenecido y abandonó

Cargo dentro de la organización (Bloque – Columna – Frente – Compañía – Guerrilla – Escuadra).

Tiempo dentro de la organización. (Años, meses, días)

Anexo E. (continuación)

Documento de Identidad (Cédula, Tarjeta Identidad, Registro Civil o Carné Sisben).

Lugar y Fecha de Nacimiento (Vereda, Corregimiento, Inspección, Municipio y Departamento).

Señales particulares (Enfermedades)

Lugar de residencia de quien efectúa presentación, en caso de que manifieste tenerla (Vereda, Corregimiento, Inspección, Municipio y Departamento). (Si aplica)

Nivel Cultural, grado obtenido, nombre del plantel y ubicación

Actividades que adelantaba antes de su ingreso a la organización.

Propiedades, cuentas bancarias, empleos.

Estado civil y nombre de cónyuge o compañera, hijos, lugar de residencia, identidad, edad, profesión, vínculos con la organización.

Nombre de los padres, lugar de residencia, identidad, edad, profesión, vínculos con la organización

Nombre de los hermanos, lugar de residencia, identidad, edad, profesión, vínculos con la organización

Nombre de familiares vinculados con la organización u otras organizaciones al margen de la ley.

Nombre de amigos, lugar de residencia, identidad, edad, profesión.

MOTIVO DE LA DESMOVILIZACIÓN.

En caso de que aplique, manifiesta que actuó como facilitador o colaborador de su desmovilización el señor(a) _____

Anexo E. (continuación)

identificado con c.c._____ Certificado con el CODA No. _____

2. **INFORME RELACIONADO CON SU PRESENTACIÓN (A los menores de edad no se les adelanta entrevista)**

Se presentó voluntariamente el _____ de _____ de 20__ en _____ en la ciudad de _____, manifestando su determinación voluntaria de abandonar sus actividades como guerrillero _____, integrante del frente _____ de la ONT _____ y acogerse a los beneficios que ofrece el Gobierno Nacional a través del Grupo de Atención Humanitaria al Desmovilizado (GAHD)

3. **ANTECEDENTES Y/O ANOTACIONES DE INTELIGENCIA.**

En el citado numeral, se debe consignar información que se posea de la persona a entrevistar, la cual debe contener datos sobre lo siguiente:

Registro en base de datos
Orden de batalla
Datos suministrados por otras fuentes (Informes de colaboradores, entrevistas otros bandoleros).

4.- **DATOS DE PSICOLOGIA**

Información sobre incorporación e ingreso a la organización armada al margen de la ley.

a. Cual fue la principal razón para ingresar a la organización.

b. Quién lo reclutó

c. A qué edad ingreso

Información de permanencia

a. Cuál es el motivo que lleva a sus compañeros a ingresar a la organización.

b. Que lo mantuvo en la organización antes de pensar en desmovilizarse

c. ¿Los cabecillas se preocupaban por su bienestar y el de sus compañeros? Explique.

d. Explique el trato (de palabra y de obra) recibido en la organización. Explique. (quién los maltrataba?)

Información sobre desmovilización

a. ¿Al cuanto tiempo de pertenecer a la organización toma la decisión de fugarse?

b. Cuáles fueron las circunstancias de tiempo, modo y lugar que lo motivaron a desmovilizarse?

c. ¿Cuál fue el factor que más incidió en Usted para tomar la decisión de abandonar la organización y desmovilizarse?

d. ¿Qué fue lo que más lo desmoralizó y desmotivó para no continuar en la organización?

e. ¿Qué recomienda para incentivar la desmovilización de sus compañeros miembros de la organización?

Debilidades y Fortalezas

a. ¿Cuál son las principales debilidades y vulnerabilidades de la organización y/o estructura a la cual perteneció? (armada, política, financiera y de convivencia entre sus miembros).

b. ¿Cuál es la principal fortaleza de la organización y/o estructura a la cual perteneció? (armada, política y de convivencia entre sus miembros)

5.- RESUMEN DE LA INFORMACIÓN

Qué actividades desempeñó antes de ingresar al grupo armado ilegal?

Proceso de acercamiento (reclutamiento) con la organización: Mecanismos empleados para tal fin.

Anexo E. (continuación)

Lugar, fecha y persona que lo reclutó.

Actividades una vez reclutado

Cursos realizados

Estructura (frente, columna, compañía) a la que fue asignado,

Cabecillas principales que conoció al ingresar al grupo armado ilegal

Armamento de dotación al ingresar

Secuencia de actividades por años a partir de su ingreso

Explique en qué consiste el plan estratégico de su organización y defina en qué fase se encuentra en la actualidad. Describa las proyecciones cercanas o a corto y mediano plazo que se trazan.

ELEMENTOS DEL ORDEN DE BATALLA

a. **DISPOSITIVO**

Ubicación:

Campamento principal, donde se encuentra el cabecilla.

Campamentos alternos o secundarios.

Desplazamientos (área de influencia y corredores de movilidad)

Veredas, municipios, sitios.

Beneficios y favorabilidades que se obtienen en las zonas fronterizas con otros países.

Anexo E. (continuación)

b. COMPOSICION

Identidad: Frente "00"

Organización: El frente en la actualidad tiene la siguiente organización:

Columnas

Compañías

Guerrillas

Escuadras

Actividades que adelantan las estructuras.

Área de influencia de cada estructura.

c. FUERZA

Hombres: El frente cuenta con aproximadamente _____ combatientes, el cabecilla principal generalmente se desplaza con la comisión de _____

Información que debe brindar sobre cabecillas:

Cabecilla Principal

N.N. (a.)

Compañera.

Anexo E. (continuación)

Grupo de seguridad,

Descripción física, y morfológica,

Enfermedades,

Sitios, frecuentados,

Arma que porta,

Medio de comunicación,

Indicativo,

Familiares dentro de la organización,

Personas de confianza,

Comportamiento y grado de aceptación en la comunidad,

Comportamiento y aceptación dentro del frente,

Contactos con integrantes del secretariado: ¿con qué frecuencia y con quiénes?

Acciones que ha planeado, dirigido o ejecutado,

Secuestros, asesinatos, hostigamientos.

Anexo E. (continuación)

¿Cuáles cabecillas han sido heridos en combate?

Debilidades y vulnerabilidades

Fortalezas

Quiénes son los principales contactos del cabecilla en los diferentes tópicos, político, financiero, apoyo, familiar o personal.

Mandos Medios

N.N. (a.)

Compañera,

Grupo de seguridad,

Descripción física, y morfológica,

Enfermedades,

Sitios, frecuentados,

Arma que porta,

Medio de comunicación,

Indicativo,

Familiares dentro de la organización,

Anexo E. (continuación)

Personas de confianza,

Comportamiento y grado de aceptación en la comunidad,

Comportamiento y aceptación dentro del frente,

Contactos con el secretariado (con qué frecuencia y con quiénes)

Acciones que ha planeado, dirigido o ejecutado,

Secuestros, asesinatos, hostigamientos.

¿Cuáles mandos medios han sido heridos en combate?

Debilidades y vulnerabilidades

Fortalezas

Quiénes son los principales contactos del cabecilla en los diferentes tópicos, político, financiero, apoyo, familiar o personal.

Guerrilleros rasos:

N.N. (a.) especialidad, arma que porta

Armas: Cantidad de armas, especificando la clase, calibre, armamento especial (misiles, morteros) y municiones.

Armamento con que cuenta la estructura:

Anexo E. (continuación)

Fusiles
Lanzagranadas
Ametralladoras
Morteros
Granadas
Otros

Equipo Especial: (Si existe algún tipo de equipo especial, visores nocturnos, miras telescópicas, geoposicionadores, otros.)

Información Sobre Menores de edad en el Frente

Cuántos menores de edad observó en el grupo armado ilegal?

Cuántos de ellos llevaban más de un año? Cuántos más de dos años?Cuántos más de 3 años, cuántos más de 5 años?

Cuántos de ellos pertenecían a alguna minoría étnica? Cuál minoría étnica?

Cuántos de ellos eran campesinos? Provenientes de qué región?

6. PROCEDIMIENTOS DELICTIVOS.

Explique los procedimientos delictivos (acciones) **que adelanta la estructura a la usted dice haber pertenecido y en los que usted participo**. Por ejemplo: secuestros, extorsiones, asesinatos, instalación de campos minados, manejo de explosivos, ajusticiamientos, retenciones ilegales de vehículos, emboscadas, plan pistolas, otros.

7. ENTRENAMIENTO

Táctico: Cursos realizados, (inteligencia, conocimiento armas y explosivos, fuerzas especiales, inteligencia urbana, comunicaciones, primeros auxilios, artillería, conductores, pilotos, planimetría, cursos exterior, técnicas).

Campamentos donde dictan la instrucción.

Anexo E. (continuación)

Instructores

Temática,

Duración del curso

Cada cuanto tiempo hay cursos,

Horarios de las instrucciones durante el curso

Elementos de ayudas de instrucción.

Ideológico: Conocimiento estatutos, textos consulta, manuales, guías de cursos, pensamiento Bolivariano, cultura general.

Técnico: manejo de equipos de sistemas, manejo Internet, intercepción de comunicaciones, otros.

8. LOGÍSTICA

Responsable e integrantes de las redes de apoyo

Ubicación de proveedores

Rutas de abastecimiento

Cada cuanto tiempo se abastecen

Ubicación de caletas

Anexo E. (continuación)

Los testaferros

Propiedades de la guerrilla que usted conoce (fincas, casas, carros, etc.)

Los talleres de _____ están ubicados en:

Tipografías

Médicos y/o enfermeros dentro del frente.

Médicos procedentes de ciudades que visitan el frente en sus áreas de influencia.

Hospitales o centros de atención clandestinos donde son atendidos los heridos y enfermos

Hable sobre el plan de salud y la consecución de medicamentos especiales utilizados por la organización y/o estructura donde usted dice pertenecía

Transportes: Vehículos, motos, carros, aeronaves, lanchas, equinos, vehículos de combate hechizos.

Equipo especial: Los uniformes camuflados, botas y elementos de uso personal,

Brazaletes

Cada cuanto tiempo les dan dotación y qué tipo de dotación,

9. EFICIENCIA DELICTIVA

Capacidades. Experiencia en combate,

Anexo E. (continuación)

Movilidad en el área,

Capacidad de concentración para ejecutar acciones conjuntas,

Apoyo de otros frentes,

Tácticas empleadas (asedio diluido, cortinas, áreas preparadas, campos minados, otros)

Infiltración o penetración en Unidades Militares y organismos del Estado.

Como se realizan las actividades de Inteligencia realizadas contra:

Unidades militares:

Estaciones de Policía:

Patrullas en el área:

Otros

Obtención de información (combate, financiera, política)

En qué consiste el manejo de masas (organización y responsables) y la capacidad de convocatoria de las mismas

Conoce usted de participación, vínculos y/o apoyos suministrados por funcionarios adscritos a entidades locales, regionales, nacionales?

Datos de interés (debilidades y vulnerabilidades)

Anexo E. (continuación)

Moral de mandos y rasos

Motivación para continuar la lucha revolucionaria

Situación afectiva,

Vicios,

Situación ideológica (charlas políticas e ideológicas y convencimiento)

Creencias religiosas

Trato con las mujeres (planificación, abusos sexuales, abortos, trabajos pesados, etc.).

Principal causa de desmovilización (deserción) de integrantes de la estructura.

Consejos revolucionarios y ajusticiamientos de bandoleros especificando detalles del mismo.

MEDIOS DE COMUNICACIÓN

Relacione los tipos, marcas, clases y descripción de los radios que emplean.

Equipo especial de sistemas:

Computadores e Internet

Como diseñan los códigos de comunicación y como es su distribución

Indicativos, frecuencias y horarios de las comunicaciones.

Cuál es lenguaje figurado más común

Conoce de la forma para cifrar y descifrar mensajes.

Anexo E. (continuación)

Qué medidas de seguridad y engaño emplean durante las comunicaciones?

Cuáles son las medidas de seguridad que toman para evitar que las Unidades Militares y de Policía los escuchen

Cuando se daña o falla un radio quien se encarga de su reparación, a donde los llevan.

Conoce la repetidora de comunicaciones.

Que clases de antena existen en el campamento.

Forma (equipos) y horario para interceptar las comunicaciones militares.

Existe emisora de su organización en el área. Explique su funcionamiento

INFORMACIÓN SOBRE INTELIGENCIA AÉREA:

¿Los campamentos bombardeados son ocupados posteriormente? ¿En cuanto tiempo?

¿Existen planes de defensa y reacción ante la presencia de aeronaves militares?

¿Cómo protegen las áreas campamentarias frente a una incursión aérea?

¿Conoce la ubicación de puestos avanzados de observación antiaérea?

¿Qué instrucción y entrenamiento reciben para contrarrestar la acción de las aeronaves militares tanto de forma diurna como nocturna?

¿Qué tipo de armamento antiaéreo poseen para atacar o contrarrestar la acción de las aeronaves militares? (cantidad lugar de adquisición y fecha).

¿Qué tipo de aeronaves poseen y como son empleadas? ¿Son propias? ¿A qué empresas o personas pertenecen?

¿Cómo están conformadas las tripulaciones? ¿Conoce nombres?

¿En qué lugar se realiza el mantenimiento? ¿Cómo adquieren los repuestos?

¿Mediante que métodos tienen acceso a las comunicaciones de las aeronaves? (frecuencias, horarios, equipos, etc.).

¿Qué pistas son utilizadas en la operación de las aeronaves?

Anexo E. (continuación)

¿Sabe si la organización recibe información de integrantes de las FAC? (Nombres, teléfonos, ubicación, caso específico, etc).

¿Ha estado presente en algún ataque de la Fuerza Aerea? ¿Qué efectos produjo este contra el grupo?

¿Conoce o ha escuchado de la existencia de misiles? (descripción cantidad, características, ubicación, fecha).

¿Cuáles son los procedimientos usados para no ser detectados por las aeronaves?

¿Se escucha claramente el perifoneo desde las aeronaves, que efectos produce?

¿Qué información conoce acerca de la Fuerza Aérea?.

¿Cómo preparan las áreas para evitar los desembarcos aéreos?

¿Qué hacen con las bombas que no estallan?

10. DATOS COMPLEMENTARIOS

Se debe consignar aspectos importantes que no estén considerados en los numerales anteriores, entre lo que se destaca (Croquis de guaridas, croquis de corredores de movilidad, Proceso de paz, ubicación fosas comunes, actores de masacres individuales y colectivas, derechos humanos, bandoleros fugados, licenciados, heridos y dados de baja.

Información sobre secuestrados

Información sobre militares y policías asesinados

Ubicación fosas comunes

a. INFORMACIÓN PARTE URBANA

Trabajo urbano del frente.

Anexo E. (continuación)

Conformación de grupos urbanos.

Integrantes grupos urbanos

Información sobre milicias

Brazo Político (PCCC – Movimiento Bolivariano), otros movimientos.

Situación del movimiento político de la organización en su área.

Métodos empleados para ganar aceptación,

Cabecillas políticos

Explique que es, quienes integran y que hacen en un:

"CER" (Comité Ejecutivo Regional),

"GEZ" "Grupo Ejecutivo De Zona"

"GER" (Grupo Ejecutivo De Radio),

Cuáles cabecillas tienen contacto con líderes políticos en la región, al interior del país o de otros países.

Cuáles políticos o personalidades visitan o tienen otro tipo de contacto con el grupo armado ilegal?

Actividades donde se hayan efectuado violaciones a los Derechos humanos.

Milicias Bolivarianas

Anexo E. (continuación)

Explique qué es y cómo se encuentran organizadas las estructuras de "milicias bolivarianas"

Relacione nombres, alias y ubicación de los integrantes de las "Milicias", material que poseen y otros datos que permitan conocer sus capacidades.

Milicias Populares

Explique qué son las milicias populares.

Relacione nombres, alias y ubicación de los integrantes de las "Milicias", material que poseen y otros datos que permitan conocer sus capacidades.

Que integrantes de este grupo de "milicianos" hicieron parte del grupo armado y porque fueron "licenciados".

b. **INFORMACIÓN SOBRE FINANZAS**

Cómo está organizada la comisión de finanzas del frente.

Cual es la actividad que vienen adelantando.

De donde obtienen las finanzas

Qué propiedades tienen los cabecillas.

Anexo E. (continuación)

Conoce algún negocio de su estructura

Qué personas o empresas aportan voluntariamente dineros a la organización.

c. INFORMACIÓN SOBRE TRÁFICO DE ARMAS

Qué contactos conoció dentro del país para la adquisición de armas, municiones o explosivos.

Conoció algún traficante extranjero que traiga armas para la guerrilla. (Datos morfológicos, etc.)

Que marcas o escudos tiene el armamento que poseen los bandoleros del frente.

Que método emplean los delincuentes para introducir armamento al país (Marítimo, Terrestre o Aéreo).

Qué rutas conoce para el transporte de material de guerra, elabore croquis, detallando puntos críticos, áreas de contacto, lugares para descanso y otros sitios de interés.

d. INFORMACIÓN SOBRE NARCOTRAFICO

Propietarios de los cultivos de coca existentes en el área de influencia de la estructura.

Ubicación de laboratorios en el área de influencia y sus propietarios.

Nombre y datos del responsable de las coordinaciones con narcotraficantes:

Anexo E. (continuación)

Que negociantes, traficantes de afuera entran al área del frente.

Elaborar croquis del sector donde se ubican los principales cultivos de coca o amapola, especificando cantidad de hectáreas cultivadas y capacidad de producción.

Igualmente diga donde se localizan los laboratorios para el procesamiento de alcaloides, elaborando croquis, que contenga: características del mismo, edificaciones existentes, capacidad de producción, sistema de seguridad, puntos críticos, vías de aproximación y escape, rutas de transporte y cantidad de personas que laboran dentro del mismo.

Qué personas de los cárteles internacionales de la droga, mantienen contacto con los cabecillas.

e. **CONTRAINTELIGENCIA**

Integrantes de unidades militares que apoyen la guerrilla,

Guerrilleros o milicianos Infiltrados en unidades militares,

Familiares de guerrilleros que trabajen en organismos del estado,

Personal retirado de los organismos del estado que le colaboren a la guerrilla.

Trabajo de inteligencia y conocimiento de instalaciones militares

Integrantes del frente que hayan pertenecido a la FFMM y a la Policía Nacional

Personal secuestrado que tenga el frente,

Anexo E. (continuación)

Fachadas para hacer inteligencia,

Integrantes de las ONGs que los visitan en los campamentos

Guerrilleros que se han desmovilizado o se han desertado,

Disidencias del frente,

Divisiones en el frente,

Conoce los planes de infiltraciones o acercamientos a las FFMM y a la Policía Nacional

Guerrilleros o familiares infiltrados en las escuelas de formación,

Personal extranjero que esta en la organización,

Que conoce sobre el plan de secuestros a personal militar,

f. **COMUNICACIONES**

a. ¿Usted ha visto o escuchado algún mensaje o propaganda de las Fuerzas Militares?

b. ¿A través de qué medio?

c. ¿A qué hora la escuchó?

d. ¿Los miembros de la organización pueden tener radio fácilmente o se les prohíbe su uso?

Anexo E. (continuación)

e. ¿Ha escuchado por la radio testimonios de miembros de la organización que se hayan desmovilizado?
f. ¿Al cuanto tiempo de desmovilizarse (otro desmovilizado conocido), usted escucho el mensaje?

g. ¿Tuvo esto alguna influencia en su decisión de desmovilizarse?

h. ¿Sintonizan la emisora del ejército?

i. ¿En qué horario la pudo escuchar?

j. ¿Qué emisoras se escuchan con frecuencia?

k. ¿Recuerda algún mensaje que le haya llamado la atención?

l. ¿Cuál?

m. ¿Qué mensaje quiere hacerle llegar a sus compañeros que aún permanecen en la organización?
n. ¿Recuerda haber escuchado o visto alguna propaganda en contra del empleo de las minas antipersonales?

o. Si la respuesta es afirmativa, explique qué impacto le causo:

1. EVALUACION DEL INFORME

Pertinencia.

A que unidad o institución es de interés.

Credibilidad

Valorar la fuente (entrevistado/individuo)

Exactitud

Valorar la información

Anexo E. (continuación)

Clasificación.

Suma de credibilidad más exactitud (letra y número)

12. INTERPRETACIÓN DE LA INFORMACIÓN

Se hace un análisis del contenido de la entrevista, resaltando los aspectos más importantes.

13. CONCLUSIONES

Se extraen los aspectos más importantes organizados por campos, como por ejemplo armado, político, financiero, otros, que sean de interés para el programa o la unidad militar o policial.

14. RECOMENDACIONES

Con base en la entrevista, se sugiere continuar el proceso en el GAHD o se recomienda ampliar la entrevista en los casos a que haya lugar.

Solicitante de proceso administrativo de desmovilización individual:
Post-firma:
Firma:
Dirección y Teléfono de un familiar:

Anexo E. (continuación)

ENTREVISTA NOMBRE Y APELLIDO DESMOVILIZADO (a.) Frente /Fecha

Entrevistador:

Código Operacional:

Nota: en el evento que el entrevistador no posea código operacional aplicaría:

Post-firma:
Firma:
Cargo:

Vo. Bo. Oficial de Inteligencia
Post-firma:
Firma

Anexo F. Auditoria y evaluación desmovilizados

MINISTERIO DE DEFENSA NACIONAL República de Colombia	FORMATO	Página 1 de 6
	INFORME SEGUIMIENTO Y EVALUACIÓN	Código: 95.1CG-MDNGGOCI8-F011-03
		Vigente a partir de: 27-AGO-2012

Auditoria N° 001	Fecha:	Día	Mes	Año
		15	01	2015

Area, Dependencia, Entidad o Proceso Auditado	Desmovilización del Grupo de Atención Humanitaria al Desmovilizado.
Establecimiento y/o lugar de la Auditoria	Grupo de Atención Humanitaria al Desmovilizado, oficina 914 edificio Bochica
Funcionario Evaluador:	TE. John Neider Orozco Gomez Ing. John Alexander Lamprea
Objetivo.	Realizar un informe de seguimiento y evaluación al proceso de Desmovilización con base en la ley 1581/2012 protección de datos personales, ley 1621/2013 y dcto 857/14
Alcance:	Realizar Seguimiento y Evaluación en el marco de la Ley de protección de datos, ley e transparencia y centro de protección de datos.
Seguimiento y Evaluación	1. Verificar el cumplimiento de la normatividad vigente en el marco de la Ley. Realizar seguimiento de ingreso al área de Desmovilización GAHD de los expedientes generados en el 2015.

Conclusiones Seguimiento y Evaluación

1. Aspecto Generales

Se realizó el informe seguimiento y evaluación, de la sección de Desmovilización del GAHD, evaluando a la sección en información general, información especifica de acuerdo marco de la Ley , así:

- Decreto 857 de mayo 02 de 2014: por el cual se reglamenta la Ley Estatutaria 1621 del 17 de abril de 2013, "por medio de la cual se expiden normas para fortalecer el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, cumplir con su misión constitucional y legal, y se dictan otras disposiciones".

Reserva legal, niveles de clasificación, sistema para la designación de los niveles de acceso a la información y desclasificación de documentos.

Articulo 6°. Protección de los documentos de inteligencia y contrainteligencia. De conformidad con la ley, los documentos de inteligencia y contrainteligencia estarán amparados, en todo momento, por la reserva legal en cualquiera de los niveles de clasificación que se les asigne. La difusión contenida en estos documentos de inteligencia y contrainteligencia observará los parámetros y restricciones consagrados en la Constitución, la Ley 1621 de 2013, el presente decreto, los manuales y protocolos que se establezcan al interior de cada organismo para su adecuada administración, protección, custodia y seguridad de la información.

Articulo 10. Reserva legal. En los términos del articulo 33 de la Ley 1621 de 2013, los documentos, información y elementos técnicos de los organismos de inteligencia y contrainteligencia estarán amparados por la reserva legal y se les asignará un nivel de clasificación de acuerdo con lo establecido en el siguiente articulo.

Articulo 11. Niveles de clasificación de la información. Los niveles de clasificación de seguridad de la información que goza de reserva legal serán los siguientes:

a) Ultrasecreto. Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar al exterior del pais los intereses del Estado o las relaciones internacionales.

b) Secreto. Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que

Anexo F. (continuación)

Conclusiones Seguimiento y Evaluación
1. Aspecto Generales
contengan información sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar al interior del país los intereses del Estado. c) Confidencial. Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar directamente las instituciones democráticas. d) Restringido. Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información de las instituciones militares, de la Policía Nacional o de los organismos y dependencias de inteligencia y contrainteligencia, sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar en las citadas instituciones y organismos, su seguridad, operaciones, medios, métodos, procedimientos, integrantes y fuentes. Artículo 12. Criterios para dar acceso a la información. Los organismos de inteligencia y contrainteligencia para dar acceso interno y externo a la información que goza de reserva legal y tenga nivel de clasificación, cumplirán con los siguientes criterios: e) Implementar de forma física y/o mediante la utilización de herramientas tecnológicas, el sistema de acceso a los diferentes niveles de clasificación, con capacidades de administración, monitoreo y control, con base en los cargos, perfiles y funciones determinadas en la estructura de cada organismo de inteligencia y contrainteligencia. Artículo 15. Centros de Protección de Datos de Inteligencia y Contrainteligencia (CPD). Los Jefes o Directores de cada uno de los organismos de inteligencia y contrainteligencia implementarán y/o adecuarán los CPD y archivos de inteligencia y contrainteligencia, designando un responsable por cada CPD en cada una de las dependencias, según su órbita funcional, nivel de clasificación de la información, desarrollo de la función en sus actividades estratégicas, operacionales o tácticas, o sus equivalentes, en cada uno de los organismos que hacen parte de la comunidad de inteligencia. • Procedimiento expediente administrativo GAHD

Anexo F. (continuación)

OBSERVACIONES GENERALES PRESENTADAS EN LA SECCIÓN DESMOVILIZADOS GAHD:

1. Se verificaron las actas diligenciadas de confidencialidad de Información, encontrando que no están firmadas por la mayoría de funcionarios.
2. En los escritorios de los funcionarios se evidencian las credenciales de autorización de manejo de información reservada de acuerdo a su función pero estas no corresponden a los funcionario actuales, se encuentran desactualizadas.
3. El área de Desmovilización en el arreglo organizacional, se encuentre organizada en el Centro Conjunto de Entrevistas, personal de Analistas Rime y la sección de producción y análisis, todas estas secciones tienen que ver o interactúan con las entrevistas del personal Desmovilizado. La sección de Analistas RIME en su mayoría son enlaces pertenecientes a las regionales de Inteligencia Militar y no son orgánicos del MDN.
4. Todos los funcionarios manejan diferentes bases de datos conformadas en Excel, para llevar el control de las entrevistas, a pesar de que existe el Sistema de Información SIGAHD, aquí solo se ingresa el concepto emitido de Voluntad y pertenencia y se consigna el material entregado por colaboración.
5. No se utiliza el Sistema de Gestión documental electrónico de Archivo, en cumplimiento a la ley de transparencia y no se carga en tiempo real los conceptos al sistema de Información del GAHD.
6. Los informes de inteligencia son clasificados de acuerdo al artículo 11 del decreto 857/2014 y se le da el correcto procedimiento, pero reposan en los pc de cada uno de los funcionarios que realizan esta actividad.
7. Los funcionarios tienen portátiles personales, no se delimita el uso de medios tecnológicos como celular y tabletas, hacen uso de los puertos USB y Unidades de CD/DVD, impresoras, discos duros externos, y escáner sin un control determinado.
8. No conocen la política de seguridad del MDN 18-2014, dejan las contraseñas en lugares visibles y/o se las prestan de acuerdo a la necesidad.
9. Los funcionarios dejan reposar gran cantidad de entrevistas sobre sus escritorios y no las evacuan conforme van llegando.
10. No se cuentan con medidas disuasivas para lograr la seguridad física.
11. Aunque se cuenta con un servicio a la entrada de la dependencia este permite el ingreso a personal de otras áreas y no toma un registro de cuál es el motivo de la visita a esta área.
12. Existe una red wifi a la cual se puede acceder sin ningún tipo de clave o contraseña, los funcionarios dicen que no saben quién es su propietario, pero que siempre la utilizan en ocasiones para el cumplimiento de sus funciones y para comunicarse con los hogares de paz y recibir la segunda entrevista.
13. No existe un plan de contingencia y de continuidad del negocio al interior de la dependencia.
14. No existe el riesgo de fuga de información en el procedimiento Expediente administrativo que interactúa con esta Área.

OPORTUNIDAD DE MEJORA

1. Crear un mecanismo de control en el área de Desmovilización, para controlar el cargue de los conceptos de Voluntad y Pertenencia
2. Emitir una circular por el Coordinador del GAHD, en el que se establezcan términos y condiciones de entrega de los expedientes desde las diferentes áreas del GAHD, teniendo en cuenta el ciclo que se dispone en la Tabla de Retención Documental y establecer la responsabilidad del área en la previa verificación de dichos expedientes.
3. Difundir e Implementar las medidas de seguridad para el ingreso al área de Desmovilización, de control de la información y documentación que repose en esta.
4. Solicitar al Coordinador de GAHD, gestionar personal y mecanismos técnicos adicionales que integre la dependencia de Desmovilización, ya que se evidencio que las metas que se deben cumplir por parte de ellos no se ajustan por la falta de los mismos.

Anexo F. (continuación)

5. Capacitar al personal en el Sistema de Gestión Documental SGDEA con el fin de que se le haga seguimiento a la información reservada y clasificada, además tener en cuenta la política de seguridad ministerial y las mejores practicas en seguridad de información coo lo son el manejo de las contraseñas.

Conclusiones del Equipo Auditor

La auditoria como principal mecanismo de seguimiento y evaluación de los procesos y procedimientos internos de la del Grupo de Atención Humanitaria al Desmovilizado, el cual conlleva de manera oportuna y completa, el análisis actual del área de Desmovilización del GAHD.

A pesar que los instrumentos de control y trazabilidad se elaboraron con las áreas, de la socialización e información de los formatos que forman parte del procedimiento de expediente administrativo, se utilizan formatos que no se encuentran autorizados, e inclusive no se utilizan los que formaron parte del plan de mejoramiento a partir de la auditoria de la Contraloria General 2013 y de control interno así como las normas de calidad, recomendando realizar una reinducción a los funcionarios encargados en cada una de las áreas, y que los responsables de área verifiquen y garanticen la utilización de los formatos aprobados.

Se sugiere que mensualmente se presente un informe por el responsable del área de los avances de los planes de contingencia y que en adelante se establezca una programación por área para la entrega, manipulación y manejo de la información para su debida organización y un plan de organización y capacitación por el área de Desmovilización.

Así mismo, se debe implementar herramientas y estrategias con el fin de sensibilizar al personal de todas las dependencias del GAHD, de la importancia del proceso de Gestión Documental.

NOMBRE COMPLETO	RESPONSABILIDAD	FIRMA
TE. JOHN NEIDER OROZCO GOMEZ	Investigador	
ING. JOHN ALEXANDER LAMPREA	Investigador	

Anexo G. Seguimiento y evaluación archivo

MINISTERIO DE DEFENSA NACIONAL República de Colombia	FORMATO	Página 1 de 6
	INFORME SEGUIMIENTO Y EVALUACIÓN	Código: 95.1CG-MDNSGOCI8-F011-03
		Vigente a partir de: 27-AGO-2012

Auditoria N° 002	Fecha:	Día	Mes	Año
		22	01	2015

Area, Dependencia, Entidad o Proceso Auditado	Archivo del Grupo de Atención Humanitaria al Desmovilizado.
Establecimiento y/o lugar de la Auditoria	Archivo del Grupo de Atención Humanitaria al Desmovilizado, oficina 914 edificio Bochica
Funcionario Evaluador:	TE. OROZCO GOMEZ JOHN NEIDER ING. JOHN ALEXANDER LAMPREA
Objetivo.	Realizar un informe en el Segundo trimestre al archivo para verificar el cumplimiento de las normas de archivo en los expedientes que se generen a partir de enero de 2014. (Un (1) informe de seguimiento), en el marco de la Ley 594 del 2000 del AGN.
Alcance:	Realizar Seguimiento y Evaluación en el marco de la Ley 594 del 2000 del AGN al archivo GAHD, que tiene en cuenta la integralidad de los documentos en su ciclo vital, comprendiendo todo el ciclo vital que sufren los documentos y expedientes del GAHD.
Seguimiento y Evaluación	1. Verificar el cumplimiento de la normatividad vigente en el marco de la Ley 594 del 2000 del AGN. 2. Realizar seguimiento de ingreso al área de archivo del GAHD de los expedientes generados en el 2015.

Conclusiones Seguimiento y Evaluación

1. Aspecto Generales

Se realizó el informe seguimiento y evaluación, al área de archivo del GAHD, evaluando a la sección en información general, información especifica de acuerdo marco de la Ley 594 del 2000 de la AGN, así:

T I T U L O I
OBJETO, AMBITO DE APLICACION, DEFINICIONES FUNDAMENTALES Y PRINCIPIOS GENERALES
ARTÍCULO 3. Definiciones. Para los efectos de esta ley se definen los siguientes conceptos, así: Archivo. Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura.
Archivo público. Conjunto de documentos pertenecientes a entidades oficiales y aquellos que se deriven de la prestación de un servicio público por entidades privadas. Archivo privado de interés público. Aquel que por su valor para la historia, la investigación, la ciencia o la cultura es de interés público y declarado como tal por el legislador.
Archivo total. Concepto que hace referencia al proceso integral de los documentos en su ciclo vital.
Documento de archivo. Registro de información producida o recibida por una entidad pública o privada en razón de sus actividades o funciones.
Función archivística. Actividades relacionadas con la totalidad del quehacer archivístico, que comprende desde la elaboración del documento hasta su eliminación o conservación permanente.
Gestión documental. Conjunto de actividades administrativas y técnicas tendientes a la planificación, manejo y organización de la documentación producida y recibida por las entidades, desde su origen hasta su destino final, con el objeto de facilitar su utilización y conservación.
Patrimonio documental. Conjunto de documentos conservados por su valor histórico o cultural. Soporte documental. Medios en los cuales se contiene la información, según los materiales empleados. Además de los archivos en papel existente los archivos audiovisuales, fotográficos, fílmicos, informáticos, orales y sonoros.
Tabla de retención documental. Listado de series con sus correspondientes tipos documentales, a las cuales se asigna el tiempo de permanencia en cada etapa del ciclo vital de los documentos. Documento original. Es la fuente primaria de información con todos los rasgos y características que permiten garantizar su autenticidad e integridad.

Anexo G. (continuación)

OBSERVACIONES GENERALES PRESENTADAS EN EL ARCHIVO GAHD:

1. Se han recepcionado 20 expedientes certificados correspondientes al acta 01 del 2015, donde se evidencio que la Secretaria Técnica del CODA, no ha entregado la totalidad de las actas correspondientes del año inmediatamente anterior

2. De los expedientes que corresponde al año 2014, se encuentra totalmente organizados y foliados quedando pendientes 381 expedientes para el proceso de digitalización.

3. No se han enviado ningún expediente a custodia de MTI, hasta que todos los documentos se encuentren debidamente organizados.

4. Se evidencio que en el área de archivo GAHD, todavia se encuentra la sección de estadistica, poniendo en riesgo la seguridad de la información. (Área de conservación. Es de uso exclusivo del personal del archivo, ya que engloba los depósitos documentales, preferiblemente en un cuerpo constructivo aislado de las otras dependencias por razones de seguridad y porque necesita unas condiciones climáticas especificas).

5. En la bodega del archivo de la oficina 906, se encuentre documentación en cajas de las áreas de Juridica y Administrativa, donde la documentación no cumple con lo minimo de estándares de calidad, de acuerdo al ***TITULO IV, ARTÍCULO 17***. Responsabilidad general de los funcionarios de archivo. Los funcionarios de archivo trabajarán sujetos a los más rigurosos principios de la ética profesional, a lo dispuesto en la Constitución Política de Colombia, especialmente en lo previsto en su articulo 15, a las leyes y disposiciones que regulen su labor. Actuarán siempre guiados por los valores de una sociedad democrática que les confie la misión de organizar, conservar y poner al servicio de la comunidad la documentación de la administración del Estado y aquella que forme parte del patrimonio documental de la Nación.

6. No existe un protocolo definido para el préstamo de información reservada y no se lleva un control de estos, pues solo se tiene un libro el cual esta desactualizado.

7. Los archivos digitalizados reposan en el pc del Responsable de la sección de archivo y usan un disco duro externo para la realización de backup.

8. Los funcionarios del archivo GAHD, no cuentan con promesa de reserva de manejo de información reservada.

9. Se evidencia que se contestan Inspecciones judiciales y se envia información por medio de correo electrónico sin ningún control, de igual manera está disponible las impresores y escáner sin una política que rija su uso.

OBSERVACIONES GERERALES ENCONTRADAS EN LOS EXPEDIENTES ANALIZADOS EN EL ARCHIVO:

1. La hoja de ruta procedimiento Gestión documental del expediente administrativo, no corresponde al formato establecido en la Suiteve Visión Empresarial, según lo evidenciado en el expediente 0057-15, de igual manera la Secretaria del CODA, no están diligenciando el paso 18 al 21.

Anexo G. (continuación)

2. El pantallazo originado por la sección de expedientes no cuenta con ningún título o nombre que pueda identificar fácilmente el documento.

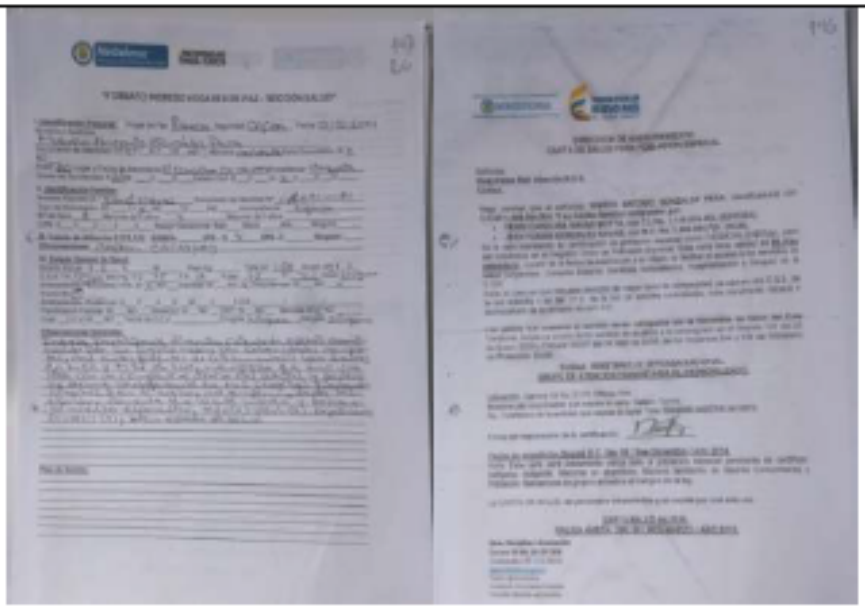
3. La ficha técnica diligenciada por los miembros del Comité Operativo para la Dejación de las Armas, no corresponde al formato establecido en la Suiteve Vision Empresarial

Anexo G. (continuación)

1. En el expediente de Atención Primeria, se evidencio que se están modificando las actas de reunión establecidas por el Ministerio de Defensa, Suiteve Vision Empresarial.

2. En el expediente de atención primaria, se evidencio que el formato de la carta de salud de población especial y el formato del ingreso de hogares de paz, no es el establecido por el GAHD en la Suiteve Visión Empresarial.

Anexo G. (continuación)



OPORTUNIDAD DE MEJORA

1. Crear un mecanismo de control en el área de Hogares de paz, para controlar la elaboración de los diferentes formatos que se diligencian en dicha área (carta de salud, acta independización), desmovilización, la Ficha Técnica, formato de ingreso a los hogares de paz, debidamente diligenciados, y firmados de acuerdo con lo establecido en la SUITE VISION EMPRESARIAL, con el fin que sea implementado de manera inmediata. Sin perjuicio de lo anterior, el área de atención primaria elaboró instructivo en cumplimiento del plan de acción en el cual se implementan los formatos del procedimiento de atención primaria cargados en el SUITEVE.
2. Emitir una circular por el Coordinador del GAHD, en el que se establezcan términos y condiciones de entrega de los expedientes desde las diferentes áreas del GAHD, teniendo en cuenta el ciclo que se dispone en la Tabla de Retención Documental y establecer la responsabilidad del área de archivo recibiendo con la previa verificación de dichos expedientes.
3. Difundir e Implementar las medidas de seguridad para el ingreso al área de archivo, de control de la información y documentación que reposa en las áreas.
4. Solicitar al área jurídica, elaborar un control del cumplimiento de las decisiones del CODA, con el fin de garantizar que se remita la información oportunamente a las autoridades judiciales o administrativas de acuerdo con lo señalado por el CODA.
5. Solicitar al área jurídica (Secretaria técnica del CODA) remitir los expedientes al área de archivo, con el fin que se avance en la organización documental, estableciendo un cronograma y metas mensuales para que el archivo cumpla con lo establecido en la Ley 594 del 2000 del AGN.
6. Solicitar al Coordinador de GAHD, gestionar personal y mecanismos técnicos adicionales que integre la dependencia de Archivo, ya que se evidencio que las metas que se deben cumplir por parte de ellos no se ajustan por la falta de los mismos.
7. Crear un protocolo de entrega de información donde se mencionen los pasos para entrega, préstamo y manipulación de la información reservada.

Anexo G. (continuación)

MINISTERIO DE DEFENSA NACIONAL República de Colombia	FORMATO	Página 6 de 6
	INFORME SEGUIMIENTO Y EVALUACIÓN	Código: 86.1CG-MONSGOCIS-F011-03
		Vigente a partir de: 27-AGO-2012

Conclusiones del Equipo Auditor

La auditoria como principal mecanismo de seguimiento y evaluación de los procesos y procedimientos internos de la del Grupo de Atención Humanitaria al Desmovilizado, el cual conlleva de manera oportuna y completa, el análisis actual del archivo del GAHD.

A pesar que los instrumentos de control y trazabilidad se elaboraron con las áreas, de la socialización e información de los formatos que forman parte del procedimiento de atención primaria, se utilizan formatos que no se encuentran autorizados, e inclusive no se utilizan los que formaron parte del plan de mejoramiento a partir de la auditoria de la Contraloria General 2013 y de control interno así como las normas de calidad, recomendando realizar una reinducción a los funcionarios encargados en cada una de las áreas, y que los responsables de área verifiquen y garanticen la utilización de los formatos aprobados.

Se sugiere que mensualmente se presente un informe por el responsable del área de archivo de los avances de los planes de contingencia y que en adelante se establezca una programación por área para la entrega de la información al archivo para su debida organización y un plan de organización y digitalización por el área de archivo.

Así mismo, se debe implementar herramientas y estrategias con el fin de sensibilizar al personal de todas las dependencias del GAHD, de la importancia del proceso de Gestión Documental.

NOMBRE COMPLETO	RESPONSABILIDAD	FIRMA
Te. Orozco Gómez John Neider	Investigador	
Ingeniero John Alexander Lamprea	Investigador	

Anexo H. Matriz riesgo – activo formato entrevista

Matriz de Análisis de Riesgo					Probabilidad de Amenaza 1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta					
	Clasificación				Confidencialidad		Integridad		Disponibilidad	
Datos e Información	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Fuga de Informacion	Acceso no autorizado al formato del sistema	Alteracion/modificacion Preguntas	Modificacion Informacion Diligenciada o ya ingresada	Destruccion	Plagio
					4	4	3	3	3	3
Documentos institucionales Formato Informe de Entrevista	x	x		4	16	16	12	12	12	12

Anexo I. Matriz riesgo – activo equipo de cómputo para entrevistas

Matriz de Análisis de Riesgo					Probabilidad de Amenaza 1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta					
	Clasificación				Confidencialidad		Integridad		Disponibilidad	
Sistemas e Infraestructura	Acceso exclusivo	Acceso ilimitado	Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Acceso a dispositivos Externos	Uso de equipos externos/personales	Uso de software no licenciado	No uso de software antivirus/antispyware	No realizacion de Mantenimiento preventivo/correctivo	Retiro e ingreso de equipos de la institucion
					4	4	4	3	3	3
Equipo para entrevistas	x			3	12	12	12	9	9	9

Anexo J. Matriz riesgo – activo entrevistador

Matriz de Análisis de Riesgo					Probabilidad de Amenaza 1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta					
	Clasificación				Confidencialidad		Integridad		Disponibilidad	
Personal	Perfil Alto, Indispensable	Perfil medio, experto en su área	Perfil bajo, no indispensable para funcionamiento institucional	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	No Existencia de actas de confidencialidad - Art38 Ley1621/2013	Error en la asignacion de Credenciales y Roles - Art36 - 37 Ley 1621/2013	Suplantacion/Reemplazo no autorizado	Amenaza/soborno/influencia externa	Ausencia de Personal capacitado para la toma de entrevista	No existencia de Unidad Militar para presentacion de desmovilizados y toma de entrevista
					3	2	4	4	4	1
Entrevistador		x		4	12	8	16	16	16	4

Anexo K. Nueva matriz riesgo – activo formato informe entrevista

Matriz de Análisis de Riesgo					Probabilidad de Amenaza 1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta					
	Clasificación				Confidencialidad		Integridad		Disponibilidad	
Datos e Información	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Fuga de Informacion	Acceso no autorizado al formato del sistema	Alteracion/modificacion Preguntas	Modificacion Informacion Diligenciada o ya ingresada	Destruccion	Plagio
					2	2	1	1	1	1
Documentos institucionales Formato Informe de Entrevista	x	x		4	8	8	4	4	4	4

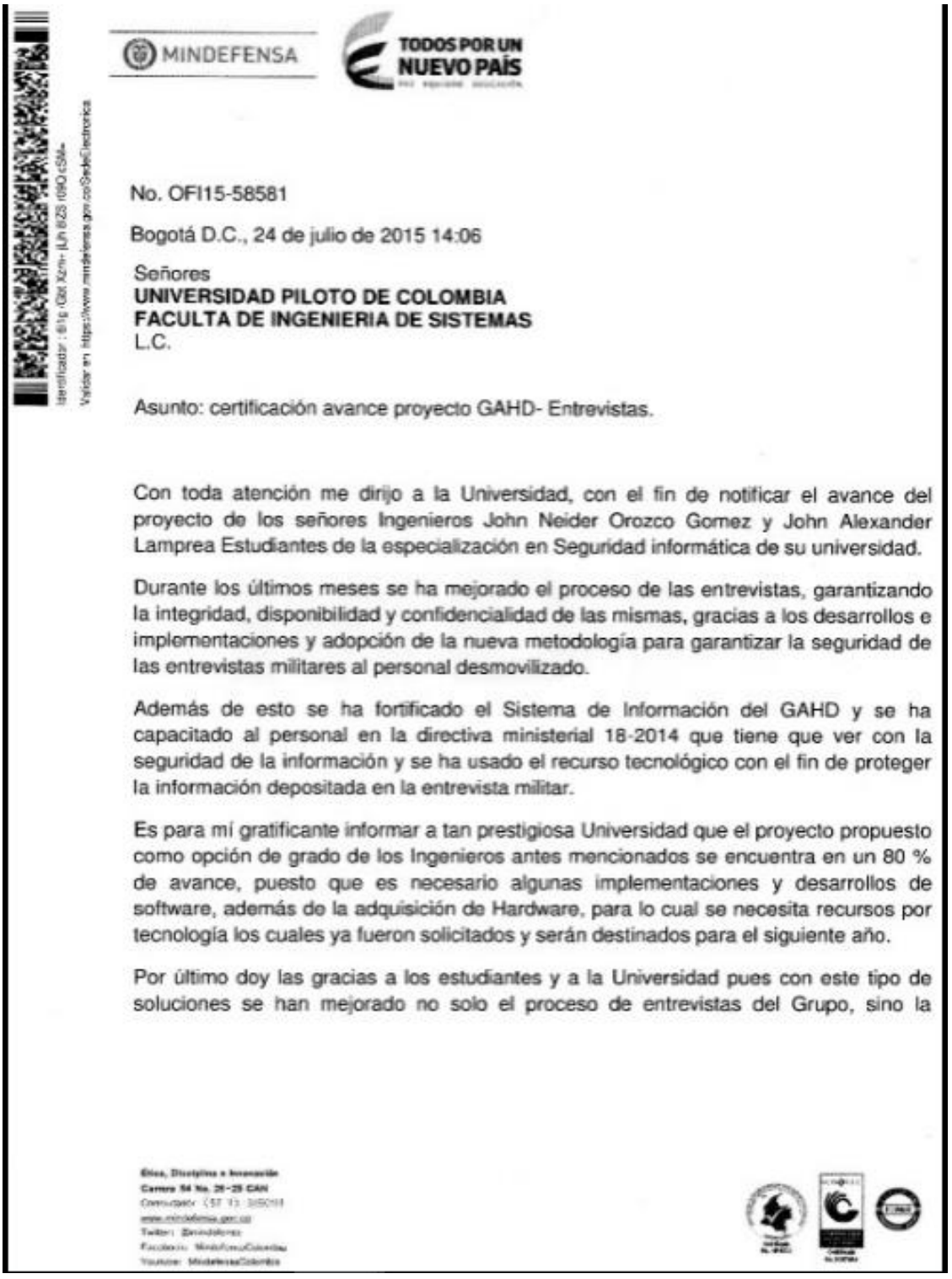
Anexo L. Nueva matriz riesgo – activo equipo de cómputo para entrevistas

Matriz de Análisis de Riesgo					Probabilidad de Amenaza 1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta					
	Clasificación				Confidencialidad		Integridad		Disponibilidad	
Sistemas e Infraestructura	Acceso exclusivo	Acceso ilimitado	Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Acceso a dispositivos Externos	Uso de equipos externos/personales	Uso de software no licenciado	No uso de software antivirus/antispyware	No realizacion de Mantenimiento preventivo/correctivo	Retiro e ingreso de equipos de la institucion
					2	2	2	1	1	1
Equipo para entrevistas	x			3	6	6	6	3	3	3

Anexo M. Nueva matriz riesgo – activo entrevistador

Matriz de Análisis de Riesgo					Probabilidad de Amenaza 1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta					
	Clasificación				Confidencialidad		Integridad		Disponibilidad	
Personal	Perfil Alto, Indispensable	Perfil medio, experto en su área	Perfil bajo, no indispensable para funcionamiento institucional	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	No Existencia de actas de confidencialidad - Art38 Ley1621/2013	Error en la asignacion de Credenciales y Roles - Art36 - 37 Ley 1621/2013	Suplantacion/Reemplazo no autorizado	Amenaza/soborno/influencia externa	Ausencia de Personal capacitado para la toma de entrevista	No existencia de Unidad Militar para presentacion de desmovilizados y toma de entrevista
					1	1	2	2	2	1
Entrevistador		x		4	4	4	8	8	8	4

Anexo N. Certificación avance proyecto GAHD – entrevistas



MINDEFENSA

TODOS POR UN NUEVO PAÍS

No. OFI15-58581

Bogotá D.C., 24 de julio de 2015 14:06

Señores
UNIVERSIDAD PILOTO DE COLOMBIA
FACULTA DE INGENIERIA DE SISTEMAS
L.C.

Asunto: certificación avance proyecto GAHD- Entrevistas.

Con toda atención me dirijo a la Universidad, con el fin de notificar el avance del proyecto de los señores Ingenieros John Neider Orozco Gomez y John Alexander Lamprea Estudiantes de la especialización en Seguridad informática de su universidad.

Durante los últimos meses se ha mejorado el proceso de las entrevistas, garantizando la integridad, disponibilidad y confidencialidad de las mismas, gracias a los desarrollos e implementaciones y adopción de la nueva metodología para garantizar la seguridad de las entrevistas militares al personal desmovilizado.

Además de esto se ha fortificado el Sistema de Información del GAHD y se ha capacitado al personal en la directiva ministerial 18-2014 que tiene que ver con la seguridad de la información y se ha usado el recurso tecnológico con el fin de proteger la información depositada en la entrevista militar.

Es para mí gratificante informar a tan prestigiosa Universidad que el proyecto propuesto como opción de grado de los Ingenieros antes mencionados se encuentra en un 80 % de avance, puesto que es necesario algunas implementaciones y desarrollos de software, además de la adquisición de Hardware, para lo cual se necesita recursos por tecnología los cuales ya fueron solicitados y serán destinados para el siguiente año.

Por último doy las gracias a los estudiantes y a la Universidad pues con este tipo de soluciones se han mejorado no solo el proceso de entrevistas del Grupo, sino la

Anexo N. (continuación)

MINDEFENSA

TODOS POR UN NUEVO PAÍS

mayoría de los procesos los cuales tienen que ver con protección de información reservada, toda vez que el presente grupo es un ente de inteligencia y muchos de los procesos debe dárseles tratamiento especial.

Gracias por su atención.

Brigadier General **MAURICIO RICARDO ZUÑIGA CAMPO**
Coordinador del Grupo de Atención Humanitaria al Desmovilizado-MDM.

Firmado digitalmente por : MAURICIO RICARDO ZUÑIGA CAMPO
Coordinador Grupo de Atención Humanitaria al Desmovilizado

Ética, Disciplina e Innovación
Carrera 54 No. 26-25 CAN
Conmutador (57 1) 3150111
www.mindefensa.gov.co
Twitter: @mindefensa
Facebook: MindefensaColombia
Youtube: MindefensaColombia

Articulo IEEE – Metodología Para La Custodia De Las Entrevistas Militares Del Personal Desmovilizado, Desde Las Unidades Tácticas De Las Fuerzas Militares Hasta El Grupo De Atención Humanitaria Al Desmovilizado

John Alexander Lamprea H, John Neider Orozco G
Universidad Piloto de Colombia
Bogotá - Colombia
John.lamprea@icloud.com
johnorozco7@hotmail.com

Resumen— Garantizar la preservación del secreto, la confidencialidad, la integridad y disponibilidad de la información suministrada en las entrevistas militares por el personal desmovilizado, demanda al grupo de atención humanitaria al desmovilizado, programa del ministerio de defensa nacional, el desarrollar una metodología para la custodia de las entrevistas militares del personal desmovilizado, desde las unidades tácticas de las fuerzas militares hasta el grupo de atención humanitaria al desmovilizado de acuerdo a la ley**.**

Índice de Términos— disponibilidad, confidencialidad, integridad, datos sensibles, metodología.

Abstract— Guarantee the preservation of the confidentiality, confidentiality, integrity and availability of the information provided in the military interviews by the demobilized personnel, demands to the group of humanitarian attention to the demobilized, program of the ministry of national defense, to develop a methodology for the custody of the military interviews of the demobilized personnel, from the tactical units of the military forces to the humanitarian group to the demobilized in accordance with the law.

Keywords— availability, confidentiality, integrity, sensitive data, methodology.

I. INTRODUCCIÓN

En el presente documento se entrega la metodología para la custodia de las entrevistas militares del personal desmovilizado, desde las unidades tácticas de las fuerzas militares hasta el grupo de atención humanitaria al desmovilizado, la cual es de suma importancia para el proceso de reintegración a la sociedad de las personas que pertenecen a grupos armados organizados al margen de la Ley (GAOML). El principal objetivo en este proyecto es permitir la actividad de entrevistas con un componente fuerte de portabilidad y comunicaciones.

Es un hecho que se necesita que esta actividad tenga unos mecanismos de control que el grupo de atención humanitaria al desmovilizado (GAHD) y en su nombre las fuerzas militares tienen interés en poder establecer, mecanismos que bajo políticas y normas permitan cumplir con las medidas de protección de la información y sus activos.

II. PLANTEAMIENTO DEL PROBLEMA

Garantizar la preservación del secreto, la confidencialidad, la integridad y disponibilidad de la información suministrada en las entrevistas militares por el personal desmovilizado, demanda al GAHD, el desarrollar una metodología para la custodia de las entrevistas militares del personal desmovilizado, desde las unidades tácticas de las fuerzas militares hasta el grupo de atención humanitaria al desmovilizado de acuerdo a la ley.

Esta información que de acuerdo a la constitución política de Colombia y a la ley 1581 del 2012 tiene carácter personal y sensible debe ser protegida por el GAHD, ya que es materia prima para definir la situación de esta población donde se mide la voluntad y la pertenencia, requisitos obligatorios para acceder a los beneficios del programa y del gobierno nacional, además también de ser un insumo necesario para el inicio de operaciones de desmovilización, donde se realiza un análisis de situación, para tratar de arrebatar la mayor cantidad de personal perteneciente a los grupos armados organizados al margen de la ley GAOML y la judicialización de los reclutadores de niños, niñas y adolescentes (NNA), disminuyendo así el enemigo y

contribuyendo de esta manera a garantizar y agilizar el proceso de PAZ y por último insumo necesario para operaciones militares, logrando así el cumplimiento de la misión institucional y constitucional de las fuerzas armadas y de policía.

El proceso de desarme, desmovilización y reintegración de personas vinculadas con los GAOML, inicia con la valoración de las circunstancias del abandono voluntario y la pertenecía a un GAOML, mediante una entrevista que se realiza inicialmente en la unidad militar y/o policial donde se presente el Desmovilizado y otra segunda entrevista que se realiza en los hogares de paz, sitio donde reside el personal desmovilizado con sus núcleos familiares e inicia el proceso psicosocial durante un lapso de 60 a 90 días.

Estas entrevistas se reportan mediante un documento, informe de entrevista el cual tiene una clasificación de reservado y contiene información exclusiva que permite constatar la pertenencia a un grupo armado ilegal y la voluntad de reincorporarse a la vida civil, y es enviada sin ningún tipo de seguridad o distribución a las oficinas del GAHD en Bogotá. D.C., en donde se recibe, se le da trámite y se le garantiza su debida custodia. Aclaramos que esta entrevista no se constituye como medio de prueba para fines judiciales.

Estas fallas de confidencialidad, autenticidad, integridad y disponibilidad de la información, han permitido que documentos clasificados como reservados hayan sido encontrados en allanamientos a personas que nada tienen que ver con organismos militares o de policía como fue el caso del nombrado hacker Andrés Sepúlveda, a quien la fiscalía general de la nación le encontró al parecer entrevistas militares con el formato del grupo de atención humanitaria al desmovilizado GAHD y bases de datos con información de personal desmovilizado.

Otro aspecto que se viene presentando con este proceso de entrevista es la falsedad en testimonio y la facilidad para entregar al desmovilizado un libreto que por su contenido le permita al desmovilizado acceder a los beneficios que le ofrece el gobierno colombiano.

Por las fallas expuestas anteriormente, es necesario esta metodología con lo cual podremos mejorar los procesos internos para el cumplimiento de la misión institucional y lo más importante garantizar el secreto al personal desmovilizado conforme a la ley.

Lo anterior manteniendo al GAHD, con los niveles de seguridad mínimos requeridos que impidan la fuga de información de las entrevistas de desmovilizados

III. MARCOS DE REFERENCIA

Autenticidad, integridad, disponibilidad y confiabilidad son conceptos ligados al manejo de la información de forma segura, que garantizan la continuidad de los sistemas de información, pero que se entiende por algo seguro, es aquello que está libre de peligro, daño o riesgo; para lograr esto es necesario el manejo de normas, procedimientos métodos y técnicas que garantizan la mínima presencia de margen de riesgo.

El Paradigma de Seguridad está cambiando; ya no es sólo asunto de protegerse de las amenazas exteriores, ahora es cuidar la información que sale, incidente que se puede ser tanto externo como interno y de forma intencional o no.

Un factor determinante en un incidente de fuga de información es la intencionalidad pues en estos casos el impacto es más claro: esa información puede ser utilizada para realizar un ataque a la organización, para venderse, para hacerse pública o para afectar la reputación o imagen de la organización, en este caso de estudio la información recibida, consignada y plasmada en el formato de entrevista al personal desmovilizado es personal e íntima, característica consagrada en el artículo 15 de la constitución política de Colombia y más allá por su expectativa de intimidad y por tratarse de datos personales está protegida por la ley 1581 del 2012, artículos 5 y 17.

Además de las características ya expuestas esta información tiene una particularidad y es que es de vital importancia para las entidades que llevan a cabo actividades de inteligencia y contrainteligencia como son las fuerzas militares y la policía nacional organizadas por éstas para tal fin, la unidad de información y análisis financiero (UIAF), la cuales están facultadas por la Ley 1621 del 17 de Abril de 2013 - Articulo 3, y que deben tratar esta información con calidad de reserva de acuerdo a lo estipulado en el artículo 33 de la misma ley.

Un actor importante en un sistema de información es el custodio y generador de la información, en este caso como todo el personal de las fuerzas militares de policía y demás organismos catalogados por la ley de inteligencia y contrainteligencia es considerado un servidor público, debe suscribir de acuerdo al artículo 38 de la ley 1621 del 17 de abril del 2013 acta de compromiso de reserva en relación con la información de que tengan conocimiento.

El manejo de esta información también está normalizado por la ley de transparencia, Ley 1712 del 06 de marzo de 2014, la cual en sus artículos 15 y 16 determina todas las obligaciones para que se tomen los programa de gestión documental en el cual se establezcan los procedimientos y lineamientos necesarios para la producción, distribución, organización, consulta y conservación de los documentos públicos.

Entendido el por qué la información del desmovilizado

debe protegerse pues es una obligación de parte del estado que las fuerzas militares, policía nacional y demás instituciones avaladas por la ley de inteligencia y contrainteligencia deben garantizar es importante integrar tecnologías que posibiliten tratar, transmitir, procesar, copiar y almacenar esta información integrándose con el factor humano el cual es el eslabón más débil de la cadena de seguridad de la información.

Estas tecnologías van desde la utilización de sistemas de data loss prevention, utilización de socket seguros SSL, redes privadas virtuales y tecnologías DLP.

IV. ESTADO DEL ARTE DEL MANEJO DE LA INFORMACIÓN DE LAS ENTREVISTAS MILITARES DEL PERSONAL DESMOVILIZADO DEL GRUPO DE ATENCIÓN HUMANITARIA AL DESMOVILIZADO

La administración del riesgo para las entidades públicas en todos sus órdenes cobra hoy mayor importancia, dado el dinamismo y los constantes cambios que el mundo globalizado de hoy exige. Estos cambios hacen que dichas entidades deban enfrentarse a factores internos y externos que pueden crear incertidumbre sobre el logro de sus objetivos.

Para afrontar esos factores se definen procesos sistemáticos, documentados y conocidos por toda la organización, enmarcados en controles específicos estructurados bajo la norma ISO/IEC 27001:2013 que permitirán identificar los riesgos a los que está sometida la información y el actuar (asumir, minimizar, transferir o controlar).

Pero para llegar a la identificación de los controles necesarios se debe realizar un análisis de brecha que permita hacer la comparación del estado y desempeño real del proceso de entrevista del desmovilizado por parte de los centros de atención al desmovilizado, teniendo como referente la normatividad legal, la metodología de riesgos de la función pública y las normas ISO27001:2013, ISO ISO27005 e ISO31000.

Este análisis se realizará en tres fases así:

A. Fase 1: Levantamiento De Información

En esta fase mediante auditorias y entrevistas se hace el levantamiento de la información que permita identificar, analizar y documentar los elementos que interactúan con la entrevista militar practicada al desmovilizado.

Esta entrevista realizada al personal de la unidad militar que recibe a la persona que desea desmovilizarse permitió conocer el proceso completo de toma de información e identificación del individuo, remisión de la carpeta hacia el GAHD, verificación del formato físico por parte del departamento de expedientes y entrega al departamento de desmovilización.

En una segunda entrevista realizada por el hogar de paz se obtiene nuevamente la información, la cual es cotejada con la ya recolectada emitiendo el concepto de voluntad y pertenencia el cual es recibido por el CODA quien en definitiva es quien toma la decisión de aprobado – aplazado o negado;

Estos procesos fueron auditados y con la información recolectada se realizó la identificación de riesgos, análisis de riesgos, valoración de riesgos para el proceso de entrevistas del personal desmovilizado del GAHD.

B. Fase II: Identificación, Análisis Y Valoración Del Riesgo Frente A La Información

El cumplimiento de objetivos de las entidades de administración pública puede verse afectado por factores internos y externos que generan riesgos frente a sus actividades, razón por la cual se hace necesario contar con acciones tendientes a administrarlos para lo cual es necesario realizar un análisis y valoración del riesgo frente a la información teniendo en cuenta su criticidad frente a la integridad, disponibilidad y confidencialidad con el fin de reducir, mitigar o eliminar su ocurrencia.

Mediante una matriz de calor y con la formula Riesgo = Probabilidad de Amenaza x Magnitud de daño, se analizaron los riesgos operativos de los activos de información identificados en el proceso de la entrevista.

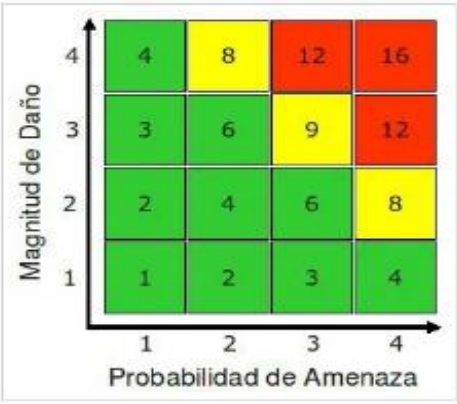


Figura. 1 – Matriz de Calor: Magnitud Daño Vs Probabilidad de Amenaza

Este análisis permitió la identificación del grado del riesgo el cual se denominó riesgo inherente, al cual se define como aquél al que se enfrenta una entidad en ausencia de acciones por parte de la dirección para modificar su probabilidad o impacto.

Cuadro 1. Análisis de riesgo promedio

		Probabilidad de Amenaza		
		Confidencialidad	Integridad	Disponibilidad
	Datos e Información	16,0	12,0	12,0
Magnitud de Daño	Sistemas e Infraestructura	12,0	10,5	9,0
	Personal	10,0	16,0	10,0

Al tratar el riesgo inherente se modifica la ponderación obtenida mediante un plan encaminado al rediseño de controles existente, diseño de nuevos controles, supresión de controles redundantes, mejora en la implementación de controles o mejora en la efectividad de los controles, obteniendo una nueva matriz que permite identificar el riesgo residual.

Cuadro 2. Nueva matriz análisis de riesgo promedio

		Probabilidad de Amenaza		
		Confidencialidad	Integridad	Disponibilidad
	Datos e Información	8	4	4
Magnitud de Daño	Sistemas e Infraestructura	6	4,5	3
	Personal	4	8	6

Esta disminución del valor del riesgo redunda en el aumento del número de desmovilizaciones individuales por el simple hecho de ser más confiables, se aumenta el poder de combate producto de la información depositada en la entrevista y su buen manejo, se aumentan las operaciones militares y de desmovilización logrando reducir los GAOML y se previene el reclutamiento ilícito

C. Fase III: Recomendaciones Administración Del Riesgo

Para lograr ese efecto transformador en el proceso de entrevistas se recomienda el re-diseño de nuevos controles, mejora en la implementación de controles y la medición de la efectividad de controles.

Todo esto encaminado a un estricto manejo y aplicabilidad de la normatividad existente, capacitación en la política de seguridad del MDN y una correcta configuración de tecnologías de información.

V. METODOLOGÍA PARA LA CUSTODIA DE LAS ENTREVISTAS MILITARES DEL PERSONAL DESMOVILIZADO

Con el fin de cumplir con los objetivos propuestos en el proyecto se diseñó una metodología para la custodia de las entrevistas militares del personal desmovilizado, la cual está confirmada por una serie de actividades que tiene por finalidad poder dar solución a los inconvenientes de seguridad presentados frente a la realización de las entrevistas.

Esta metodología cubre las actividades a desarrollar teniendo en cuenta los aspectos normativos, tecnológicos, de talento humano y entorno, focos a partir de los cuales se diseñarán medidas y procedimientos claros que junto con la política general será de estricto cumplimiento.

Su alcance es aplicable en su totalidad a las unidades tácticas de las fuerzas militares y al Grupo de Atención Humanitaria al Desmovilizado y su verificación y seguimiento estará a cargo del jefe del Área de Desmovilización, Jefe del Área de Atención Primaria.

VI. CONCLUSIONES

Es de vital importancia para una organización, que los funcionarios conozcan las políticas que rigen la misma y las implicaciones que conllevan el desacato de una directriz. La seguridad es de todos, y por lo tanto se deben unir esfuerzos para atacar en los diferentes flancos los riesgos a los cuales puede estar expuesta una institución en un momento dado, además de implementar controles y medidas disuasivas y prever el futuro.

RECONOCIMIENTOS

Ingeniero John Jairo Echeverry Aristizabal – Tutor Temático

Brigadier General Mauricio Ricardo Zuñiga Campo -

Coordinador Grupo de Atención Humanitaria al Desmovilizado.

REFERENCIAS

[1] Administración de Riesgos Corporativos. Técnicas de Aplicación PricewaterhouseCoopers, Colombia. 2005. Página 39.
[2] ARANTXA Calvo Moyano. Fuga de información, la mayor amenaza para la reputación corporativa. [on line]. [Fecha de consulta 24 enero de 2016]. Disponible en: http://www.redseguridad.com/opinion/articulos/fuga-de-informacion-la-mayor-amenaza-para-la-reputacion-corporativa
[3]. GUTIÉRREZ Amaya Camilo. 10 años de fuga de información: conoce los incidentes para no repetir la historia. – ESET. [on line]. [Fecha de Consulta: 16 de enero del 2016]. Disponible en http://www.welivesecurity.com/la-es/2015/01/08/10-anos-fuga-de-informacion/

Autores

John Alexander Lamprea Hernández.
Ingeniero de Sistemas.
Aspirante al título de Especialista en Seguridad Informática
Universidad Piloto de Colombia.

John Neider Orozco Gómez
Ingeniero de Sistemas.
Aspirante al título de Especialista en Seguridad Informática
Universidad Piloto de Colombia.